Table of Contents

Chapter 1: About Probe Instances................................................................................................. 5
   Introducing Probes..........................................................................................................................5
   What is a probe instance?................................................................................................................6
   Which software probe is right for you?..........................................................................................8
   How probes work with switches....................................................................................................10

Chapter 2: Expert Probe Software............................................................................................... 12
   How to install or upgrade the software........................................................................................12
   Comparing software probe features............................................................................................13
   Minimum and recommended system specifications.................................................................15
   How to upgrade to Windows 10....................................................................................................16
   How to install all versions.............................................................................................................16
   How to upgrade version 17 and later..........................................................................................17
   How to upgrade version 16 and earlier.......................................................................................17
   Capture card driver requirements...............................................................................................17
   Installing the wireless NIC driver on Windows 7/Vista..........................................................18
   Installing a third-party USB wireless adapter..........................................................................19
   Installing Windows updates and updating virus protection.................................................20

Upgrading the probe software......................................................................................................21
   Upgrading the probe software directly......................................................................................21
   FAQ: Licensing and updating.....................................................................................................21
   Backing up your GigaStor settings.............................................................................................23

Creating a probe instance.............................................................................................................24
   Creating GigaStor active and passive probe instances..........................................................26
   Creating and configuring an MPLS probe instance....................................................................27
   How to use additional storage volumes on the GigaStor active instance..............................27

Connecting to a Probe..................................................................................................................27
   How to change the monitored network adapter.........................................................................27
Chapter 1: About Probe Instances

Introducing Probes

Discover the basics of probes, probe instances and what type is right for you, and how probes work with switches.

As a network administrator, when something goes wrong on your network, seeing what is happening on the wire can quickly lead you to a solution. Use this guide to assist you with choosing, deploying, configuring, and using your probes. The probes, along with Observer Analyzer software, let you see all traffic on the network to which it is connected. To monitor multiple networks from a single analyzer, probes must be installed at every point where network visibility is required.

Probes collect and report network traffic and statistics (usually from a switch) to an Observer. This enables you to detect and anticipate problems on both local and remote portions of the network. Probes gain insight and visibility into every part of the network, access remote networks as easily as local networks, eliminate the time and expense of traveling to remote sites, and speed troubleshooting.

A probe is a hardware device on your network running VIAVI probe instance software. Each hardware probe has at least one probe instance that captures packets from your network to analyze. The probe hardware device could be an appliance purchased from VIAVI or you could install the probe software on your own hardware.

The probe can be located on the same system as the analyzer (every Observer includes a “local probe”), or the probe can communicate with remote analyzers over TCP/IP.
Probes monitor the following topologies:

- 10/100 Mb, 1/10/40 Gb Ethernet (half- and full-duplex)
- Wireless (802.11 a/b/g/n)

**Figure 1 (page 6)** shows how probes provide visibility into your network. It may be obvious, but it also shows that you cannot see traffic on portions of your network where you do not have a probe. Finally, you can put Observer anywhere on your network so long as it has TCP connectivity to the probe.

**Figure 1: Typical network**

---

**What is a probe instance?**

Observer has only one kind of probe instance: the **probe instance**. If you have a GigaStor then you have two special probe instance types available to you: the **active probe instance** and the **passive probe instance**.

Observer uses probes to capture network data. In some cases you may want or need more than one probe in a specific location. You can achieve that through probe instances. A probe instance provides you the ability to look at multiple network interfaces, have multiple views of the same interface, or to publish to multiple Observer.

**Table 1 (page 6)** compares the features of active and passive probe instances with an Observer probe instance found on all non-GigaStor probes.

**Table 1. Active vs. passive GigaStor instances and Observer probe**

<table>
<thead>
<tr>
<th>Better suited for troubleshooting</th>
<th>GigaStor Active probe instance</th>
<th>GigaStor Passive probe instance</th>
<th>Observer Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better suited for data capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Start packet capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Stop packet capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Start GigaStor packet capture</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
A passive probe instance may capture packets to RAM and allows you to do reactive analysis or look at real-time statistics for troubleshooting. The passive probe instance binds to a virtual adapter or a network adapter that has data coming to it that you want to capture. You can change whichever adapter a passive probe instance is bound to without affecting any active probe instance. By default a passive probe instance uses 12 MB of RAM. You can reserve more memory for passive probe instances if you wish.

**Caution:** With a GigaStor you have the option of which NIC to bind the passive probe instance. Do not bind any passive probe instances to the capture card adapter if at all possible. A copy of all packets is sent from the adapter to every passive probe instance attached to it. If you have several passive probe instances attached to the capture card adapter, the capture card’s performance is significantly affected. Instead attach the passive probe instances to either a 10/100/1000 adapter or to a non-existent one.

If you have a passive probe instance connected to a GigaStor, you can mine data that has already been written to the RAID disk by using an active probe instance. There should be one passive probe instance for each simultaneous Observer user on a GigaStor. By using a passive probe instance, instead of an active probe instance, only one copy of data is being captured and written to disk, which reduces the processor load and the required storage space. For troubleshooting and most uses in Observer passive probe instances are appropriate.

An active probe instance on a GigaStor captures network traffic and writes it to the RAID array. An active probe instance should have as large of a RAM buffer as possible to cushion between the network throughput rate and the array write rate. Like a passive probe instance, it can also be used to mine data from the hard disk, however a passive instance is better suited for the task. An active probe instance cannot start a packet capture while the GigaStor Control Panel is open.

By default there is one active probe instance for GigaStor. It binds to the network adapter and its ports. If you have a specific need to separate the adapter’s ports and monitor them separately, you can do so through passive probe instances or you can create separate virtual adapters.

- Only one active probe instance per GigaStor.
- Set scheduling to Always for the active probe instance so that it is constantly capturing and writing data. Use a passive probe instance to mine the data.
Do not pre-filter, unless you know exactly what you want to capture. Of course, if something occurs outside the bounds of the filter, you will not have the data in the GigaStor.

Do not allow remote users access to the active probe instance.

Figure 2: GigaStor capture and packet capture through probe instances

Figure 2 (page 8) shows how one active probe instance captures and writes to the GigaStor RAID. Passive probe instances 1 and 2 mine data from the RAID array. As a best practice, the passive probe instances are bound to the slowest network adapter in the GigaStor.

Additionally, passive probe instance 3 and 4 are each capturing packets separate from each other and separate from the active probe instance. However, since they are also bound to the same adapter as the active probe instance, they are capturing the same data as the active probe instance.

Which software probe is right for you?

Software probes are an economical choice for many situations.

For companies that cannot invest in dedicated hardware probes, Observer Platform software probes provide a low-cost monitoring option and are easy to install and configure. Software probes support Ethernet, Gigabit and wireless and are appropriate for analyzing speeds of up to 1000 Mbps or for low-utilization gigabit networks via a SPAN/mirror port on a switch. The Observer software can handle fast network speeds (including 40 Gigabit), but it is the network adapter that is the bottleneck on home-grown systems. VIAVI uses a custom-designed
Introducing Probes

Chapter 1: About Probe Instances

network adapter removing the bottleneck in our probes. These levels of software probes are available:

- Single probe—Single probes have only one probe instance and it is not user-configurable. Single probes are appropriate for sites with small administrative staffs where only one user needs to look at a probe at a time.

- Multi Probe—Multi probes may have one or more probe instances. Multi probes allow multiple users to each connect to the probe and use their own probe instance. Each probe instance can be looking at the same packet capture or different capture.

- Expert probe—Expert probes are the same as a Multi probe except that they have local expert analysis and decode capabilities in the probe that allows for remote decoding and expert analysis in real time. The Expert probe software comes pre-installed on most hardware probes from VIAVI.

<table>
<thead>
<tr>
<th>Hardware &gt;</th>
<th>Installed software &gt;</th>
<th>GigaStor, Portable probes, Probe Appliances, 3rd party hardware</th>
<th>Dual port Ethernet Probe, 3rd party hardware</th>
<th>Ethernet Single probe, 3rd party hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends entire buffer(^1)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarms</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trending</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Triggers</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Encrypts buffer transfer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Simultaneous multi-topology support</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simultaneous users(^2)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports multiple NICs (page 34)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use reserved memory outside of Windows (page 35)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated reporting with Apex</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Able to switch between probe and analyzer mode (page 49)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full-duplex(^3)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS (page 27)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## How probes work with switches

The purpose of a switch is to isolate traffic to the local network, thereby reducing the amount of traffic each device on that network must see and process. Although a protocol analyzer puts a network interface card in "promiscuous" mode, the analyzer only sees packets addressed to or transmitted from the port that it is connected to on the switch.

To operate a probe in a switched environment, you must choose a method that provides network visibility to the port where the probe is connected. Most switches provide a function that "mirrors" all packets received or transmitted from either a single port of interest (for instance, a server or router), or multiple ports of interest. The mirrored traffic can then be captured or analyzed by connecting your analyzer (or in this case, the probe) to the "mirror port" (which is sometimes called a SPAN port).

### Note:

Switches typically provide two options for configuring the SPAN/mirror port settings. You can either use a command line interface (CLI) or web-based interface included with your switch to set the port (or ports) to be mirrored.

To SPAN/mirror ports, Observer can use SNMP to directly query your switch and report port-based statistics or use RMON to report any internal RMON statistics the switch may have. Selecting the method right for you depends on your switch, and the level of detail you need to troubleshoot the problem at hand. For packet capture, decode and Expert Event identification, only static port

<table>
<thead>
<tr>
<th>Hardware &gt;</th>
<th>GigaStor, Portable probes, Probes Appliances, 3rd party hardware</th>
<th>Dual port Ethernet Probe, 3rd party hardware</th>
<th>Ethernet Single probe, 3rd party hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software &gt;</td>
<td>Expert Probe</td>
<td>Multi Probe</td>
<td>Single Probe</td>
</tr>
<tr>
<td>NetFlow (page 62)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port bonding (page 59)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote decode of GigaStor captures</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sends expert summary &amp; decode packets</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP expert, APA, ATA (page 49)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Buffers are sent to Observer where the decoding and analysis is performed. This is less efficient than sending the expert summary and decode packets, which is available with Expert Probe.
2. Simultaneous users are supported when each user has his own probe instance.
3. Only available on hardware probes from VIAVI.
4. Decoding and expert analysis are performed by the probe and a summary is sent to Observer reducing network bandwidth use.
5. Application Performance Analysis and Application Transaction Analysis. Applications are generally OSI Layer7 applications like HTTP, FTP, RTSP, SMB, and so on.
mirroring provides all the information required for a complete picture of what is happening on your network.
Chapter 2: Expert Probe Software

Observer needs a probe to capture network traffic. The probe can be local to Observer Analyzer or remote.

How to install or upgrade the software

This section describes the installation process and minimum requirements if you are installing Observer or probe on your system. This applies to physical and virtualized servers. If you virtualize the server, each server must meet these specifications.

**Prerequisite(s):**

- An administrator account is required to install and run any version of Observer or probe software except Observer Expert Console Only (ECO). Observer ECO requires an administrator account just for installation; a standard user account can be used for running Observer ECO.
- Standard network cards do not support “raw” wireless packets, nor do they enable “promiscuous” mode by default. Promiscuous mode captures all packets for the analyzer, not just those addressed to the network card. Both “raw” wireless packets and promiscuous mode are required by Observer. ErrorTrak drivers were needed in earlier versions of Observer. They are no longer necessary.
- If you do not meet the minimum requirements, the system may seem to operate in the short term, but be aware that even if a sub-minimum installation works momentarily, a later, heavier load on the system can cause it to fail. VIAVI sells hardware probes that are guaranteed to keep up with heavy loads. See the Observer Platform website for details.
- You may install the probe software on a virtual machine so long as it meets the system requirements. The installation process is the same. You may also want to consider using a virtual TAP.
**Caution:** See the important information in How to upgrade to Windows 10 (page 16) if you want to upgrade the operating system!

1. Ensure your system meets the minimum requirements.
   See Minimum and recommended system specifications (page 15).

2. Choose one of the following:
   - How to install all versions (page 16)
   - How to upgrade version 17 and later (page 17)
   - How to upgrade version 16 and earlier (page 17)

After completing this task:
   - License your software. See FAQ: Licensing and updating (page 21).

### Comparing software probe features

Single Probes are appropriate for sites with smaller administrative staffs. This type of probe communicates with only one Observer at a time.

If you have a need for multiple network administrators to view packet decodes and analysis from the same probe simultaneously, choose a Multi Probe. The Multi Probe allows you to run multiple probe instances of the probe on a single system, which means that:

- You can install multiple network interface cards in a single Multi Probe system, allowing multiple “points of visibility” from that probe.
- You can connect multiple sessions of Observer to the same Multi Probe system. Any Observer session can see all of the networks available on the Multi Probe. The probe instances are securely encrypted and password-protected.

Although Multi Probes behave similarly to Single Probes, the Multi Probe has a different user interface for configuring the probe.

For the highest level of distributed performance, choose an Expert Probe. An Expert Probe provides Expert Analysis and capture/decode capabilities. This saves bandwidth when performing remote expert analysis, and also allows remote decode views and expert analysis in real time.

The Expert Probe can be configured to run as an Observer when you need to perform troubleshooting from where the probe is located.

<table>
<thead>
<tr>
<th>Hardware &gt;</th>
<th>GigaStor, Portable probes, Probe Appliances, 3rd party hardware</th>
<th>Dual port Ethernet Probe, 3rd party hardware</th>
<th>Ethernet Single probe, 3rd party hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed software &gt;</td>
<td>Expert Probe</td>
<td>Multi Probe</td>
<td>Single Probe</td>
</tr>
<tr>
<td>Sends entire buffer</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarms</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Trending</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Triggers</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
1. Buffers are sent to Observer where the decoding and analysis is performed. This is less efficient than sending the expert summary and decode packets, which is available with Expert Probe.

2. Simultaneous users are supported when each user has his own probe instance.

3. Only available on hardware probes from VIAVI.

4. Decoding and expert analysis are performed by the probe and a summary is sent to Observer reducing network bandwidth use.

5. Application Performance Analysis and Application Transaction Analysis. Applications are generally OSI Layer7 applications like HTTP, FTP, RTSP, SMB, and so on.
Minimum and recommended system specifications

If you are installing the software on your own hardware or a virtual machine, these are the minimum and recommended specifications for a production environment.

Table 2. Observer Expert Console Only (ECO)

<table>
<thead>
<tr>
<th>Processor / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dual core Pentium class processor</td>
<td>Quad core Pentium class processor</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB RAM</td>
<td>8 GB RAM</td>
</tr>
<tr>
<td>Operating system</td>
<td>64-bit Operating System Windows 7 or newer</td>
<td>64-bit Operating System Windows 7 or newer</td>
</tr>
<tr>
<td>Network Card</td>
<td>Server-class</td>
<td>Intel server-class</td>
</tr>
</tbody>
</table>

1. If your system has 4 GB of RAM, you cannot reserve any memory for Observer. This is a limitation of Windows known as the BIOS memory hole. Either add more RAM or take some out.
2. See Supported Operating Systems (page 16) for a full list of supported operating systems.

Table 3. Observer or GigaStor Software Edition in a virtual server

<table>
<thead>
<tr>
<th>Processor / CPU</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Four core</td>
<td>Six core Intel</td>
</tr>
<tr>
<td>RAM</td>
<td>Minimum 16 GB (8 GB for Observer and 8 GB for the operating system)</td>
<td>64 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>Packet capture - Hardware: Determined by your product</td>
<td>Same</td>
</tr>
<tr>
<td></td>
<td>Packet capture - GigaStor Software Edition: Determined by your license.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network trending: See  .</td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td>64-bit Operating System Windows 7 or newer</td>
<td>64-bit Operating System Windows 7 or newer</td>
</tr>
<tr>
<td>Network Card</td>
<td>Virtualized network adapter</td>
<td>Intel server-class</td>
</tr>
<tr>
<td>Capture Card</td>
<td>Virtualized network adapter</td>
<td>Server-class onboard network adapter</td>
</tr>
</tbody>
</table>

1. If your system has 4 GB of RAM, you cannot reserve any memory for Observer. This is a limitation of Windows known as the BIOS memory hole. Either add more RAM or take some out.
2. See Supported Operating Systems (page 16) for a full list of supported operating systems.
3. A second network card that acts solely as a capture card is required (and must be in “promiscuous mode”). Alternatively, a dual-port NIC can be used.

Current compatibility and incompatibility of virtual machines with the GigaStor Software Edition (GSE) is described in this list:

- VMWare ESXi Server
  - ESXi 5.0 and higher is compatible with GSE.
- VMWare Workstation Pro is not supported with GSE
- Microsoft Hyper-V may function but is not supported with GSE
Supported Operating Systems

Your product must be installed on one of these operating systems to receive assistance from Technical Support.

<table>
<thead>
<tr>
<th>Product name</th>
<th>64-bit Windows</th>
<th>32-bit Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 (SP1 or higher) or newer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2008 R2 Enterprise, Standard, Web (SP1 or higher) or newer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 7 (SP1 or higher) or newer</td>
<td>Not supported</td>
<td></td>
</tr>
</tbody>
</table>

How to upgrade to Windows 10

Due to the way Microsoft has designed its Windows® 10 operating system upgrade feature, Expert Probe will not function if you upgrade your operating system from Windows 7, Vista or Windows 8 to Windows 10 without first uninstalling Expert Probe.

This information does not apply if you:
- Already uninstalled Expert Probe.
- Are installing Windows 10 rather than upgrading to it.
- Are already using Windows 10.
- Are upgrading using the Observer Platform OS Upgrade product because it replaces the operating system rather than upgrading it. Additionally, it uses Windows Server 2012 R2.

**Note:** Unfortunately, if you have already upgraded the operating system and Expert Probe was not uninstalled prior to upgrading to Windows 10, the only path to recovery is to reinstall the operating system. Back up any Expert Probe files on the operating system, reinstall the operating system, then install Expert Probe and restore its files.

To upgrade a system with Expert Probe to Windows 10:

1. Back up your settings.
3. Upgrade your operating system.
4. Install the Expert Probe software.
5. Restore your settings from step 1 using whatever method is best for you.

Expert Probe is now available to use on Windows 10.

How to install all versions

Use this procedure to install all versions of the software.

**Prerequisite(s):**
An administrator account is required to install and run any version of Observer or probe software except Observer ECO. Observer ECO requires an administrator
account just for installation; a standard user account can be used for running Observer ECO.

1. Insert the installation CD in your CD drive or use the latest installation image from our update site. If you copied the installation files from our web site, start the installation program.
   
   http://update.viavisolutions.com/latest/ObserverSetupx64.exe

2. When the setup program runs, follow the onscreen instructions.

3. Choose to install:
   - Observer.
   - Advanced Probe. Choose this for Single Probe or Multi Probe. Your license determines whether it is a Single Probe or Multi Probe.
   - Expert Probe

4. After the files have been installed on your system you must restart Windows. You will not be able to run the software until you restart your computer.

How to upgrade version 17 and later

Version 17 allows you to upgrade directly from within Observer or from OMS (if used).

If OMS is not controlling Observer, then do the following in Observer:

If OMS is controlling Observer:

The software is updated to the latest version.

How to upgrade version 16 and earlier

Upgrading version 16 uses the same procedure as installing the software. The process is different for version 17 and later.

1. Insert the installation CD in your CD drive or use the latest installation image from our update site. If you copied the installation files from our web site, start the installation program.

   http://update.viavisolutions.com/latest/ObserverSetupx64.exe

2. When the setup program runs, follow the onscreen instructions.

3. Choose to install:
   - Observer.
   - Advanced Probe. Choose this for Single Probe or Multi Probe. Your license determines whether it is a Single Probe or Multi Probe.
   - Expert Probe

4. After the files have been installed on your system you must restart Windows. You will not be able to run the software until you restart your computer.

Capture card driver requirements

If you are going to use a third-party capture card in your probe, the capture card must meet certain requirements so that Observer can report statistics and errors.
The network card used to monitor or capture network traffic must have all of the mandatory and optional NDIS functions. The VIAVI capture card has all of the necessary features.

Most NIC vendors provide solid, functional NDIS drivers for all cards available within the Ethernet, Token Ring, and FDDI marketplace.

Accessing a standard network with a “normal” network device is somewhat different from what a protocol analyzer requires. While both share a number of driver functions, a protocol analyzer requires a set of features and functions that the average network device will never need. Examples of these optional functions are promiscuous mode, error tracking, and network speed reporting. (Examples of mandatory functions would include functions to determine the maximum packet size, functions to verify the number of sent packets, and functions to specify or determine a packets’ protocol.)

Microsoft made a number of the less used (by “normal” network users) functions “optional”, as opposed to “mandatory” regarding driver requirements. The result has been that most vendors support all (or most) mandatory functions with the first release of the driver. As time passes, and the initial chaos of the first release of the card and driver passes, most manufacturers add some or all of the optional functions, as well as fix or complete all of the mandatory functions.

As part of the optional section of defined NDIS functions, Microsoft specified a number of counters that can be kept for Ethernet frame errors. These counters include CRC errors, Alignment errors, Packets Too Big (Jabbers), and Packets Too Small (Runts). Collisions are counted, but there are limitations of NDIS collision statistics. Four important points should be considered:

- These optional counts only provide a numerical value to the total number of errors on the segment (i.e. the number of CRC errors found), they do not specify where (which station) the error originated from.
- After the error packet is identified and the proper error counter is incremented, the packet is discarded, and not sent to Windows (this is the reason it is impossible to determine the source of an Ethernet error packet with standard NDIS drivers).
- A number of vendor’s NDIS drivers return a positive acknowledgment when the NDIS error function is queried for existence, but the error statistic is not actually kept.
- A few vendors (3COM, for example) do not keep any error statistics whatsoever.

If a NIC driver both reports that the optional Ethernet error statistics are being kept, and actually keeps data on these errors, Observer reports these statistics in the Network Vital Sign Display.

### Installing the wireless NIC driver on Windows 7/Vista

See the information in Monitoring a wireless access point (page 50), which contains details about raw packets and promiscuous mode for the network card.

Follow these instructions to install the wireless driver for your network card:

1. Click **Start** and then right-click on the ‘Computer’ icon and choose Properties.
2. Click Device Manager.
3. Right-click on the wireless adapter you want to use as your capture card and choose Update Driver Software.
4. Choose “Browse my computer for driver software.”
5. Choose “Let me pick from a list of drivers on my computer.”
6. Click Have Disk and use the drivers in this location:
   
   Example: C:\Program Files\Observer\DRIVERS\Wireless\Atheros_Vista

7. Click Next and Windows installs the driver for your wireless card.

   To confirm that you correctly installed the driver for the wireless network card, open Observer. If the probe instance shows (Wireless) behind it, then it is correctly configured.

   Figure 3: Probe instance using wireless adapter

   If the probe instance shows (Ethernet), then either the network card driver was not correctly installed or the probe instance is not configured to use that network card. You can confirm the correct network card is selected, by choosing Actions > Select Network Adapter Card.

   After completing this task:
   
   ♦ License your probe by following the instructions in Licensing and updating (page 21).
   ♦ If your wireless network uses an encryption key, you must add the encryption key information. See Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling (page 35).

Installing a third-party USB wireless adapter

You can capture wireless 802.11 traffic on systems lacking built-in wireless by installing a third-party USB wireless adapter. Wireless access point statistics and other features become usable as well. Installing a special driver on your USB wireless adapter is necessary.

Prerequisite(s):

The USB wireless adapter is only supported on systems running Windows Vista or 7 (32- or 64-bit).

Caution: For some wireless adapters you must install the software for the USB wireless adapter before you attach the adapter to your computer. This is not an Observer requirement, but one of the wireless adapter. If you attach the USB wireless adapter before installing the software, unplug the USB adapter, uninstall the software, restart your system, and then proceed with step 1.
Note: If using a Belkin N600DB USB wireless adapter, only revision number “F9L1101v1” is compatible. These adapters have a Broadcom chipset. The second revision, “F9L1101v2” does not have a Broadcom chipset and is incompatible.

1. Install the software that came with your USB wireless adapter.
2. Insert the USB wireless adapter into your system.
3. Choose Control Panel > Network and Sharing Center > Change adapter settings and then select your USB wireless adapter. Right-click and choose Properties.
4. From the Networking tab, click Install > Service > Add. Click Have Disk and locate this file: NiNdisMon.inf
   - 64-bit: C:\Program Files\Observer\DRIVERS\Wireless
   - 32-bit: C:\Program Files (x86)\Observer\DRIVERS\Wireless
5. Click OK to install the software as a Windows service.
6. Restart your system.
   Restarting allows the software and adapter to be fully recognized by your system and the Windows service to start. Observer will not be able to use the wireless adapter until you restart.
7. Start Observer, select the probe instance you want to associate with the USB wireless adapter.
8. Choose the USB wireless adapter you just installed.
   The probe instance is now configured to use the USB wireless adapter. You can confirm this because the word "[Wireless]" appears after the probe instance name, and the Wireless 802.11 tab of the probe instance is visible.

Installing Windows updates and updating virus protection

From time to time Microsoft releases updates for the operating system used for your probe or your virus protection software vendor updates their virus definitions. You should apply those updates as soon as feasible, however, you should always apply the updates manually.

We do not recommend that you allow Windows to automatically install the updates and restart the system. By manually applying the updates you ensure that the system restarts properly and that the probe starts correctly whether running as a Windows service or as an application.

For your anti-virus software, follow these guidelines:

- Ensure TCP ports 25901 and 25903 are open. All Observer Platform products communicate on these ports.
- Ensure UDP ports 25901 and 25903 are open if you use OMS.
- For all probes, disable any scanning of the Observer installation directory (typically C:\Program Files\Observer) and of D: (RAID) drive as scanning greatly diminishes the performance of writing data to disk.
- The performance of the operating system may be greatly diminished when using anti-virus software.
Upgrading the probe software

Observer and probe software must be within the same major release. This may require you to upgrade your probe software.

If the version of Observer or GigaStor that you are upgrading was installed on a 32-bit operating system and you have upgraded the operating system to 64-bit, the installer upgrades existing installation to 64-bit version keeping the same path.

Version 17 requires a 64-bit operating system. If you previously installed a 32-bit version, the same installation directory is used.

Use information from this section when upgrading to a new major version of the probe software. Before upgrading have the following available:

- Your probe license information.

Note: If you are using encryption keys with Observer, you can continue to use your existing keys or transfer them to your probe (and analyzer) as necessary.

Upgrading the probe software directly

On the probe:

1. Start the Observer installation program.
2. Follow the on-screen instructions and choose your probe type.
3. After the installer completes, restart the system.
   - New major builds may have new drivers or other files that require a restart.
4. Connect the probe to an Observer.

FAQ: Licensing and updating

Some customer concerns deal with licensing and updating issues. Explore this good resource for licensing and updating help, or call the Technical Support department for further assistance.

How to license Observer and GigaStor

To license and activate a compatible GigaStor, Observer, or Probe:

2. After launching the application in DEMO mode, click the Help menu and select License Observer.
3. Click the Enter Name button in the lower left corner.
4. Type into the Contact/Department and Company boxes exactly what is listed in your license document.
5. Click OK, and then click Accept on the confirmation dialog.
6. Ensure the Identification Number matches the number on your license document. If they do not match, click Re-Type Name? to correct any mistakes.
7. Type the license number, from your license document, into the License Number box.

How to update your license

If Observer or GigaStor is already licensed and you need to modify, update, or change that license, you can do so.

Prerequisite(s):
This task requires you have already licensed (page 21) your Observer or GigaStor.

This task cannot be completed if the license to your Observer or GigaStor is managed by OMS. Instead, refer to.

Updating your license refers to changing, editing, or updating the license that is already applied to your product. Some reasons for needing to do this can include:

♦ Activating a new license. The new license might provide different or increased functionality over your existing license, like increased data storage for a GigaStor Software Edition (GSE).
♦ Changing a license. Perhaps you accidentally applied the wrong license to your product and need to change it.

To update a license:
2. Click OK to confirm you want to re-license.
3. Type the license number, from your license document, into the License Number box.
4. Click the Re-Type Name? button in the lower left corner.
5. Type into the Contact/Department and Company boxes exactly what is listed in your license document.
6. Click OK, and then click OK on the confirmation dialog.

You successfully updated your license. Observer begins using the license the next time Observer is launched.

Close and restart Observer for the new license to take effect. You may need to coordinate a suitable time to do so if restarting would affect many users or significantly interrupt your data collection.

Why is my license number not working?

Each license number is case-sensitive, so be sure to type it in exactly the way it was given to you. Also, if you copy-pasted the license number into the activation prompt, be sure you did not introduce a leading or trailing space character—those are not part of your license number.

Ensure you are licensing the correct version of Observer. License numbers are version-specific. License numbers work within equal major version numbers of the product only. For example, an 17.0 license can be used to activate 17.x versions but not 16.1, 16.0, 15.1, 15.0, etc.

Could I have my license re-sent to me?

Yes. If you lost the original information containing your license number, please contact us so we can resend your license document(s).
What type of license do I have?

The type of license you have is described in your license document. Each license document contains a license number, and the document describes which software version the license number applies to. If it does not, or you notice any other error, please call our support team for assistance.

Should I uninstall Observer before updating it?

If you wish to update your existing Observer software to a newly released version within the same major release number, you do not need to uninstall your existing version for the update process to succeed. Simply install the new version over the old.

Backing up your GigaStor settings

You can back up most Observer settings and configuration data. Backups are useful when migrating to new hardware, upgrading the operating system, or recovering from data loss.

Caution: If you are using data encryption on your GigaStor system, you must save the encryption keys before upgrading the operating system. Because the keys are typically stored on the operating system drive, they will be lost during the upgrade process. If you do not have a copy of the keys elsewhere, you will not be able to access stored data (packets) after the upgrade is complete.

Your Observer may not have each directory referenced in this topic, but you can back up those that are present. Use whatever backup method is best for you.

To back up many Observer settings and files, do the following:

- Copy the files and directories in Table 4 (page 23) to a backup location. This must be a location other than the operating system drive of the system you are planning to upgrade.

Table 4. Directory or files to back up

<table>
<thead>
<tr>
<th>Directory or file</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network Trending  | C:\Program Files\Observer\NetworkTrending  
                    This contains your Network Trending data. If you have changed the default location for Network Trending data, you must back up the new location. Use the Folders tab in to verify which folder is used for trending data. |
| Protocol Definitions | C:\Program Files\Observer\ProtocolDefs  
                        This contains any modifications or additions you have made to the protocol definitions list for each probe instance. Back up in all cases. |
| Multicast Definitions | C:\Program Files\Observer\MulticastDefinitions  
                         This contains the templates for defining trading multicast streams for Network Trending. Back up if you use trading multicasts in Network Trending. |
| Settings | C:\Program Files\Observer\Settings  
                  This contains alarms and triggers. Back up if you heavily use alarms or have alarm/trigger customizations that need to be retained. |
<table>
<thead>
<tr>
<th>Directory or file</th>
<th>Description</th>
</tr>
</thead>
</table>
| SNORT Rules      | C:\Program Files\Observer\Forensics  
                 | This contains your SNORT information, such as rules, for detecting malicious activity in your packet captures. Back up if you use SNORT. |
| Expert Thresholds | C:\Program Files\Observer\ExpertSettings  
                   | This contains your thresholds stored in Expert settings. These include TCP/UDP events and some triggers for problem identification. Back up if you have modified any Expert thresholds and want to retain those customizations. |
| SNMP             | C:\Program Files\Observer\SNMP  
                   | This contains any custom MIBs, compiled MIBs, request files and SNMP trending data. Back up if you have made SNMP changes or have SNMP trending data. Use the Folders tab in to verify which folder is used for SNMP. |
| Address Tables   | C:\Program Files\Observer\LocalAddressTable  
                   | This contains your Discover Network Names list. Back up if you have run Discover Network Names and have saved the alias list.  
                   | C:\Program Files\Observer\ProbeAddressTable  
                   | This contains the Discover Network Names list from any remote probe that has connected to this Observer analyzer. Back up if you have run remote Discover Network Names and saved the alias list. |
| Scripts          | C:\Program Files\Observer\Scripts  
                   | This contains the scripts for Observer. Back up if you have created or modified a script. |
| Windows Registry | Using Regedit, export the following registry branch:  
                   | 32-bit Windows operating system running any version, or 64-bit Windows operating system running version 16 or higher:  
                   | HKEY_LOCAL_MACHINE\SOFTWARE\Network Instruments |
| License          | Make note of the license information in . You need the contact/department, company, identification number, and license number. |

### Creating a probe instance

You can create a probe instance to monitor network traffic seen on a network adapter, explore saved packet captures, and have multiple people be able to see the captured data from their copy of Observer. Create a passive or active probe instance depending on what your goals are.

**Prerequisite:** Multi or Expert Probe.

When you open Expert Probe for the first time, you assign memory to a probe instance. You can choose to use this one probe instance, or you can create other probe instances. Multiple probe instances are useful if you need multiple users using the same probe simultaneously or if you have specific needs for each probe instance (for instance, packet capture, trending, and so on). See Configuring connections to multiple NICs or Observer (page 34) for why you would want to use multiple probe instances.
To set up a probe instance, follow these steps:

1. Do one of the following:
   - On the probe: Click the **Adapters and Redirection tab**.
   - In Observer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the **Adapters and Redirection tab**.

2. In the upper left, click New Instance. The Edit Probe Instance wizard opens.
   - If the New Instance button is grayed out, it probably means you do not have enough Observer-allocated memory to add another instance.
   - If you get a message that says that there is not enough reserved memory to create a probe instance, you must reduce the amount of memory used by another probe instance. By default all of the reserved memory on a GigaStor is assigned to the “Instance 1” active instance. By releasing some of the reserved memory you re-allocate memory from one probe to the pool of reserved memory from which you can create other probe instances, including passive probe instances on the GigaStor. Click the **Configure Memory** button and reduce the amount of memory for the packet capture buffer.
   - You must have a minimum of 256 MB RAM to run the probe with a single instance, plus 12 MB for each additional probe instance. See **Setting the total system memory reserved for probes** (page 35) for details on allocating memory for Observer probes.

3. Ensure “Probe” is selected in the Instance type. Type a name and description and click **Next**.

4. Choose an appropriate capture buffer size given the local system’s available memory and how much traffic you plan on capturing from the given network.
   - Statistical reporting uses different memory—and much less of it—than packet capture.
   - Although it is possible to customize the amounts of memory used by various Observer statistical displays (by choosing a statistics memory configuration), for most situations the defaults work perfectly well. For additional information, see **Customizing statistics and capture buffers for probe instances** (page 33).
      a. If you need to create your own memory configuration, click New. The New Statistics Memory Configuration window opens.
      b. Type a name and choose a default memory configuration to use. Click Finish. After choosing the memory configuration, you can change how the memory is allocated.
      c. Select your newly created memory configuration and click Edit. The Edit Statistics Memory Configuration window opens.
Creating a probe instance

d. Choose your network type. For each Observer statistic, choose how much memory is allocated for it. Click **OK**.

e. Click **Next** to continue, and the Select Network Adapter and Redirection configuration dialog is displayed

5. Ensure the correct network adapter is selected and type the IP address of your Observer. Click Finish.

Creating GigaStor active and passive probe instances

**Prerequisite:** Expert Probe

GigaStor probe instance creation is only available when you are using the Expert Probe *locally* on a GigaStor probe and with the program in application mode, not as a Windows service. It is not available if you connect to the Expert Probe from a remote Observer analyzer.

If your GigaStor RAID has more than 256 TB, see How to use additional storage volumes on the GigaStor active instance (page 27) before continuing.

By default, the GigaStor has an active probe instance called "Instance 1" but does not have any passive probe instances. We recommend that you

- Rename the active probe instance by selecting Instance 1 and clicking Rename. Choose a name that is meaningful to you for the probe instance name and click **OK**. A typical name might be the physical location of this GigaStor.
- Have only one active GigaStor instance, unless you have specific reasons to have more.
- Create passive probe instances to use.
- See details about active and passive probe instances discussed in What is a probe instance? (page 6).
- After creating your active instance, if you want to change how much disk space is reserved for that active instance, click Configure Instance Storage.

To create a passive probe instance, follow the steps in Creating a probe instance (page 24). When you create a probe instance for an Expert Probe on GigaStor, it is automatically created as a passive probe instance.

If you want to change a passive probe instance to an active probe instance, follow these steps.

1. Do one of the following:
   - On the GigaStor probe: Click the **GigaStor Instances tab**.
   - In Observer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the **GigaStor Instances tab**.

2. Select the passive probe instance you want to promote to an active instance and right-click.

3. Choose Make Instance Active. Your passive probe instance is now an active probe instance.

After completing this task:

You should then create passive probe instances for it.
Creating and configuring an MPLS probe instance

**Prerequisite:** Expert Probe

See Creating a probe instance (page 24) for details about creating an MPLS probe instance. In Creating a probe instance (page 24) choose MPLS Probe and follow the on screen instructions.

After the probe instance is created, you may want to configure the probe to tell it what type of traffic is seen.

2. On the General tab, use the options in the MPLS Analysis Settings to choose whether Observer should auto determine IPv4 and IPv6, what all other traffic is (ATM or Mac Header), and whether to use a four byte pseudowire word.

3. Click OK.

How to use additional storage volumes on the GigaStor active instance

When expanding your RAID array beyond 256 TB of usable disk space, you must add the additional volumes to your GigaStor active instance.

**Prerequisite:** Expert Probe

The maximum NTFS disk volume is 256 TB, but with a GigaStor you can have more storage than that by using the expanded disk arrays or striping through Windows.

1. On the GigaStor probe, click the **GigaStor Instances** tab.
2. Select the **Use additional storage volumes** option and click **Configure**.
3. In the message box that appears, click **Yes**.
4. Select the additional storage volumes you want to assign to your active probe instance, and click **OK**.
5. In the message box that appears, click **Yes**.

The additional storage is allocated. This may take a few moments.

**Connecting to a Probe**

You can connect to a probe from multiple direction: from or to a different Observer analyzer, to its own probe instance (connect to itself), and change the network adapter that is monitored on each probe instance.

**How to change the monitored network adapter**

If your probe has multiple network cards in it, you can choose which card you want to monitor.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on VIAVI or third party hardware.

**Note:** If you have a network card in your system, but it is not being seen or recognized by Observer, follow the instructions in No network adapter available (page 104).
Tip! If you are seeing only broadcast traffic, you do not have the correct network card selected or you do not have your switch port configured correctly as a SPAN/mirror port. Change the network adapter you are monitoring or configure the SPAN/mirror port.

- When choosing the monitored adapter from within Observer for all probe versions:
  1. In the probes list, select the probe instance.
  2. Choose .
      The **Select Network Adapter** window appears.
  3. Select the network adapter you want to monitor, and click **Select**.

- When choosing the monitored adapter on the probe for Multi Probe and Expert Probe:
  1. Click **Adapters and Redirection**.
  2. Select your probe instance and click **Configure Adapter/Redirection**.
      The **Edit Probe Instance** window appears.
  3. In the **Selected Network Adapter** area, change the network card you are monitoring.
      The probe instance is now using the newly selected adapter.

### Connecting to a probe for the first time from Observer

2. Click **New** to add the probe to the Probe Administration and Redirection list.
3. Type the IP address that you assigned to the probe and click **OK**. You may leave the other fields blank. If you type a name, the name will change after Observer connects to the probe. The probe appears in the list of available probes.
4. Select the probe and then click Redirect Selected Probe.
5. Select the probe instance and click Redirect Selected Instance.
6. Choose the “Redirect to this Observer” option, then click the **Redirect** button. Within 30 seconds the probe will connect with the analyzer.

Probe redirection can be password protected or disabled. Please see Connecting the Multi Probe or Expert Probe to an Observer (page 28) for details. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa (page 103). After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling (page 35).

7. Close the Probe Instance Redirection window.

### Connecting the Multi Probe or Expert Probe to an Observer

**Prerequisite:** Multi or Expert Probe.

There are two ways to connect the probe to an Observer. The method described here is from the perspective of the probe. All actions are done on the probe itself.

Each probe instance can be connected to only one Observer at a time. Connecting the probe instance with the analyzer is called “redirecting” it. This is because the probe instance may not be connected to any Observer or it may be connected to
a different Observer than the one you want to connect it to. The connection can be done from within the analyzer or from the probe. This section describes how to redirect a probe instance from the probe and assumes that the probe software is running and that you already have a probe instance.

1. Click the **Adapters and Redirection tab**.
2. Select the probe instance you want to redirect and click the **Configure Adapter/Redirection** button at the top. The Edit Probe Instance window opens.
3. Select the “Redirect to a specified IP address or DNS name” option and provide the IP address or DNS name. When the probe instance is connected, the “Redirected to” column lists the IP address of Observer system. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa (page 103).
4. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling (page 35).

### Connecting to a probe instance from an Observer analyzer

**Prerequisite:** Multi or Expert Probe.

Probe instances can be redirected from one Observer to another or disconnected from any analyzer. This is done from Observer.

1. Select the probe instance you want to redirect and click the **Redirect Selected Probe Instance** button at the bottom. The Edit Probe Instance window opens.
2. If this is the first time you are connecting to the probe from Observer, you must add the probe to your list. See Connecting to a probe for the first time from Observer (page 28).
3. If the probe is not connecting, Probe redirection might be password protected or disabled. Please see Connecting the Multi Probe or Expert Probe to an Observer (page 28) for details. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa (page 103).
4. After the probe is connected, see Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling (page 35).

### Connecting the probe to an Observer

There are two ways to connect the probe to an Observer. The method described here shows you from the perspective of the probe. The second way is described in Connecting the Multi Probe or Expert Probe to an Observer (page 28). All actions are done on the probe itself.

1. Choose **Options > Probe Redirection Settings**. The Probe Redirection Settings dialog opens.
2. Use **Table** to complete the settings. If the probe is not connecting, see A probe is not connecting to the analyzer or vice versa (page 103).

<table>
<thead>
<tr>
<th>Observer IP address</th>
<th>Type the address of Observer you want this probe to connect to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Probe redirection for remote users</td>
<td>Allows remote users to redirect the probe to their Observer. If you want the probe to be able to connect to only one Observer, leave this option unchecked.</td>
</tr>
<tr>
<td>User name</td>
<td>By default any user can connect to the probe and no password is required.</td>
</tr>
</tbody>
</table>
Redirecting a probe instance

Your local Observer may already have local probe instances defined, but you can add numerous remote probes, including GigaStor, too. You must first redirect the remote probe to your local Observer.

A probe may have multiple probe instances, which are useful if you need multiple users using the same probe simultaneously or if you have specific needs for each probe instance (for instance, packet capture, trending, and so on). When you connect to a probe, ensure you select the probe instance you need and not one being used by someone else.

**Note:** Probe redirection can either be password protected or disabled, depending on the target probe.

To redirect a probe instance, complete the following steps:

2. Do one of the following:
   - If you see a remote probe instance you want to redirect, skip directly to step 6.
   - If your list is empty or missing the remote probe instance you want to redirect, proceed to step 3.

3. Click **New**.

   The **Edit Remote Probe Entry** dialog appears.

4. Type the IP address, or DNS address, of the remote probe.

   If you type a DNS name, it resolves to its IP address.

5. If necessary for probe access, type a user name and password, and click **OK**.
6. Select the remote probe instance from the list, and click **Redirect Selected Probe Instance(s)**.

Allow time for the remote probe to redirect. How long this operation can take is limited by a timeout countdown.

The probe instances of the remote probe are shown.

7. Select a probe instance from the list, and click **Redirect Selected Instance**.

8. Select the **Redirect to this Observer**, and click the **Redirect** button.
9. Close the **Probe Instance Redirection** window.

If the operation succeeds, the remote probe instance is now redirected to the local Observer. Now you can use the remote probe instance just as you would if it was running on your local machine.

## Configuring a probe's name and other probe options

Set the probe network adapter speed, reserve system memory for probes, configure connections to multiple network adapters, set “always on” traffic capture, customize statistic and capture buffers, and more.

**Prerequisite(s):**

These steps assume you are viewing the probe interface, which is the only choice when using Expert Probe software. But if you are using a GigaStor, ensure that you are viewing the probe interface (page 49).

The probe has many options that you can configure.

1. **Choose Options > Probe Options.** The Probe Options dialog opens, which lets you configure the probe.
2. **Use this table to complete the settings.**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe name</td>
<td>Allows you to specify a name for the probe which appears in Observer probe list. The default name is a random mix of numbers and letters. We suggest renaming the probe to something meaningful to you. The name may be its physical location or any other standard you choose. The probe name</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Trending folder</td>
<td>Allows you to specify where the network trending data is saved. The default is C:\Program Files\Observer \NetworkTrending. Unless you have a specific reason to use another directory, we suggest using the default.</td>
</tr>
<tr>
<td>Folder for GigaStor</td>
<td>Allows you to specify where the GigaStor and network packet data will be saved. The default is C:\Program Files\Observer \Data if a software install or non-GigaStor probe or D:\Data if a GigaStor hardware appliance. Unless you have a specific reason to use another directory, we suggest using the default.</td>
</tr>
<tr>
<td>Maximum IP DNS resolution entries</td>
<td>Defines the maximum number of DNS entries the probe should maintain. The probe will keep up to the number of entries defined or what the probe can maintain in 10 MB of storage space, whichever is less. The probe keeps the first 10,000 entries (or whatever amount you define) it sees; it does not keep a rolling list of the last 10,000. After the limit is reached, no more entries are kept. They are discarded.</td>
</tr>
<tr>
<td>Run Probe as Windows Service</td>
<td>Select this option if you want to run the probe as a Windows service. This allows the probe to start without requiring a user to log in and start the probe. The probe starts whenever the system starts, which can be especially important for a remote probe. The change takes effect on the next system restart.</td>
</tr>
<tr>
<td>View certificates from other Observer assets</td>
<td>Click the Certificates button to view trusted, untrusted, and pending trust, certificates that allow secure asset-to-asset communication. See Understanding the certificate trust model for details.</td>
</tr>
</tbody>
</table>

### Customizing statistics and capture buffers for probe instances

**Prerequisite:** Multi or Expert Probe.

Before changing any of the buffer sizes, you should understand how any changes you make affects the probe. See How a probe uses RAM (page 64).

- To change memory allocation for probe instances, see Running (page 69) Observer (page 69) with reserved memory (page 69).
- To fine-tune the Statistics Memory Configuration, see How to adjust the statistical buffer.
Configuring probes to collect data even when not connected to an analyzer

Probes (and probe instances) can be configured to collect data only when you tell it to—including manually starting/stopping the collection, having collection always running, or based on a schedule. The schedule and settings are saved with the probe instance. This means if you choose to have packet capture always running or running on a schedule that the probe instance does not need to be connected to an Observer.

To configure when packet capture should run, complete these steps:

1. In Observer, select a probe instance in the Probes list.
2. Click the **Settings** button. The Packet Capture Settings window opens.
3. Click the **Schedule tab**.
4. Choose the schedule you want (Always, daily, or specific days).
5. If you want to control the capture buffer’s size, click the **Capture Options tab**. The data is saved on the probe in C:\Program Files\Observer\Data.

Setting the probe’s time clock synchronization settings

At times your capture card drivers time clock may drift. They can be synchronized with the system clock, if you wish. Unless you notice a reason to enable this feature, we recommend that you do not synchronize your capture card’s time clock.

Some Other things to consider:
- The capture card synchronizes itself with the system clock at when the system starts.
- Generally, you are interested in relative time between packets, not the actual time a packet was seen.

1. Do one of the following:
   - On the probe: Click the **Synchronization tab**.
   - In Observer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the **Synchronization tab**.
2. Click the **Edit Schedule** button.
3. Choose when and how you want the capture card’s time clock to synchronize with the system clock and click **OK**.

Configuring connections to multiple NICs or Observer

**Prerequisite:** Multi or Expert Probe.

With a Multi Probe, you can configure the probe to view multiple networks if multiple NICs are installed on the local system and to provide multiple Observer with views of the local network interfaces.

The probe accomplishes these capabilities by allowing multiple instances of itself. A probe instance is a virtual probe with attributes that define:
- Which network interface on the local system to capture data from.
- Which Observer (local or remote) to direct the data to.
Setting the total system memory reserved for probes

**Prerequisite:** Multi or Expert Probe.

Memory use is an important and vital part of using an Observer probe successfully. Before changing any of the reserved memory, you should understand how any changes you make affects the probe.

Configuring the probe’s adapter speed, ToS/QoS precedence, and statistics sampling

After connecting the probe instance to Observer Analyzer, there still may be some additional configuration that you must do. This is completely dependent on your network environment and your needs.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on VIAVI or third party hardware.

In Observer:

1. Select a probe instance in the Probes list.
2. Right-click and choose **Probe or Device Properties**.
3. Use the following tabs to further configure the probe for your environment. Not all of these tabs are present at all times. What tabs are visible depends on the type of probe you are configuring. For instance, the Gigabit tab is only visible when you are configuring a Gigabit Probe. For details about the fields on each tab, see the Configuring a probe's name and other probe options (page 32).

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Set the statistics sampling divider and MPLS settings. For field descriptions, see Probe Properties field-level descriptions (page 36).</td>
</tr>
<tr>
<td>Adapter speed</td>
<td>Verify that the adapter speed is registering correctly. Change the adapter speed if necessary. Changing the adapter speed here may be useful and necessary, because statistics, graphs, and reports generated by Observer are set using the adapter speed as the maximum. If, for some reason, Observer is not able to correctly identify your adapter speed your reports may be inaccurate. For field descriptions, see Probe Properties field-level descriptions (page 36).</td>
</tr>
<tr>
<td>ToS/QoS</td>
<td>Ensure these settings match your needs paying particular attention to the IP precedence bit for the ToS/QoS of your network. What you set here affects how the Observer analyzer displays information about VoIP, NetFlow, sFlow, and capture decodes. For field descriptions, see Probe Properties field-level descriptions (page 36).</td>
</tr>
<tr>
<td>Gigabit</td>
<td>Define the maximum frame size for your network. The default is 1514 bytes (excluding the frame checksum), which is appropriate for standard Ethernet. If the network link you are analyzing is configured to support jumbo frames (frames larger than 1514 bytes), you may want to change this setting to match the frame size of the Gigabit network, up to a maximum size of 9014 bytes. Observer will then discard frames that exceed this maximum frame size, generating a &quot;Frame too large&quot; error.</td>
</tr>
</tbody>
</table>
Your probe instance is now configured. You can begin collecting network traffic and statistics using it. Typically, this is done in Observer by choosing Capture > Packet Capture and clicking the Start button. See Configuring probes to collect data even when not connected to an analyzer (page 34) for details. You do not, however, need to start a packet capture to see statistics. See the list of statistics available under the Statistics menu in Observer.

**Probe Properties field-level descriptions**

This section include details about many of the fields and options for a probe.

### Table 5. General tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication timeout</strong></td>
<td>Allows you to define how long Observer will wait for the Probe to communicate before it assumes the connection is lost. Values are from 2 to 60 seconds.</td>
</tr>
<tr>
<td><strong>Probe report period or local Observer information refresh time</strong></td>
<td>Allows you to set how often the Probe sends a refresh packet or how often the local Observer’s dialogs are refreshed. This value has a minimum of 2 seconds with no maximum.</td>
</tr>
<tr>
<td><strong>Statistics report (refresh) period</strong></td>
<td>Allows you to set the statistics display refresh period. This value has a minimum of three seconds with no maximum.</td>
</tr>
<tr>
<td><strong>Vital signs report (refresh) period</strong></td>
<td>Allows you to set the Network Vital Signs refresh period. Values are from 10 to 600 seconds.</td>
</tr>
<tr>
<td><strong>Sampling Divider</strong></td>
<td>On probes with less processing power, high traffic rates (such as those typical of gigabit connections) can overwhelm the probe’s ability to keep up. A sampling divider tells Observer to only consider one of every n packets when calculating statistical displays, where n is the sampling divider. This setting only affects statistical displays such as Top Talkers, Internet Observer, etc. (packet captures are unaffected). A sampling divider of 2...</td>
</tr>
</tbody>
</table>
### Configuring a probe's name and other probe options

#### Chapter 2: Expert Probe Software

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>registers every other packet; a sampling divider of 10 registers every tenth packet. Some statistical displays consider every packet regardless of this setting. Bandwidth Utilization looks at traffic as whole, so does Wireless Site Survey.</td>
<td></td>
</tr>
</tbody>
</table>

Encapsulated Traffic Analysis

| Encapsulated Traffic Analysis | GRE (Generic Routing Encapsulation) and GTP (GPRS Tunneling Protocol) are two encapsulation protocols that may have been deployed on your network. To show the encapsulation IP addresses, leave the box unchecked; to show the nested IP addresses, check the box. This setting also applies to L2TP and IPv4. |

Nortel OEL2 Metro Ethernet Analysis Settings

| Nortel OEL2 Metro Ethernet Analysis Settings | Choose if frame headers should be analyzed as OEL2 headers. |

MPLS Analysis Settings

| MPLS Analysis Settings | Choose whether Observer should auto determine IPv4 and IPv6, what all other traffic is (ATM or Mac Header), and whether to use a four byte pseudowire word. Also choose whether to use the MAC addresses from encapsulated MPLS header. |

---

### Table 6. Parameters tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network type</td>
<td>Displays the probe's network topology, such as Ethernet, Token Ring, wireless, and WAN.</td>
</tr>
</tbody>
</table>

**Network speed**

| Network speed | Displays the network speed. The distinction here is between the actual, measured speed of the network and the speed that the NIC card, possibly incorrectly, reads from its connection. For example, a 10/100Mb NIC card on a 10/100Mb connection to a switch on a network where all the other stations are running at 10Mb will report the network speed as 100Mb. This item is the actual number that the NIC card driver sends Observer, so 10Mb Ethernet will be reported as 10,000,000. 100Mb Ethernet will be reported as 100,000,000. |

**NIC card name**

| NIC card name | Displays the name of the card as reported by the NDIS driver to the registry. |

**Probe version**

| Probe version | Displays the probe version used by the local Observer or probe. |

**Number of adapters**

| Number of adapters | Displays the number of cards the local Observer or probe has configured. |

**Instance memory (MB) and Capture Buffer (MB)**

| Instance memory (MB) and Capture Buffer (MB) | Displays the amount of RAM the instance or probe has available for statistics and capture buffer. Observer has no limitations on the amount of RAM that can be used for a buffer. The maximum allowable buffer size is displayed in the Options > Selected Probe or SNMP Device Properties > Probe Parameters tab. |

**View Probe Instance Memory Allocation**

| View Probe Instance Memory Allocation | Lets you view and edit how the memory used for statistics is allocated for this probe instance. |

**Network errors Supported by the NIC NDIS driver**

| Network errors Supported by the NIC NDIS driver | Displays the aggregate errors that your NDIS driver provides statistics for. |

---

### Table 7. Adapter Speed tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Network Speed</td>
<td>Your current speed reported by the network card.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Adapter Speed</td>
<td>Choose to let Observer and the NIC automatically determine the network speed, or to select from various values (in megabits per second) for the network speed to be used for calculations. The primary use of this is to correct a mistaken NIC’s impression of overall network speed. A network card connected to a 10 megabit hub on a gigabit network will think that the entire network is only 1% as fast as it actually is.</td>
</tr>
</tbody>
</table>

Table 8. Autoupgrade tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoupgrade probe within minor version release</td>
<td>Activates the autoupdate feature for minor version (i.e., point) releases (which do not require a new license).</td>
</tr>
<tr>
<td>Autoupgrade probe for major version release</td>
<td>Activates the autoupdate feature for major version releases. You must supply an ID and license key to update probes with a major version release.</td>
</tr>
<tr>
<td></td>
<td>If the probe includes a capture card and the upgrade includes a Field Programmable Gate Array (FPGA) firmware update, the system must be manually shut down and restarted before the firmware update can take effect. A system restart will not complete the firmware upgrade (a shut down is required); however, the autoupgrade process will restart the probe system, thus completing the probe software upgrade. In most cases, the probe will still be operable with a software-only upgrade, but any of the benefits of the firmware update are not activated until you manually shut down and restart the probe.</td>
</tr>
<tr>
<td>Force Probe Autoupgrade to the current Observer version</td>
<td>This provides a manual mechanism for updating a probe.</td>
</tr>
</tbody>
</table>

Table 9. ToS/QoS tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect Protocol Distribution by QoS</td>
<td>When enabled, QoS data is collected.</td>
</tr>
<tr>
<td>Use 802.11e Wireless TID/QoS</td>
<td>When enabled, QoS for wireless networks is collected.</td>
</tr>
<tr>
<td>IP ToS/QoS Standard User Defined</td>
<td>This tab is used for NetFlow and VoIP analysis. IPv4 supports the Type of Service (ToS) byte, also known as the Precedence byte. Different RFCs define different ways to interpret the byte: Default (RFCs 1349, 1195, 1123, and 791) OSPF V2 (RFCs 1248 and 1247) DSCP (RFC 2474) User Defined The information on the right shows the bit assignments. User-defined interpretations are also allowed. for the currently selected option. The User defined option displays entry fields that allow you to define the meaning of each bit position in the ToS byte.</td>
</tr>
</tbody>
</table>
Configuring a probe’s name and other probe options

Chapter 2: Expert Probe Software

Table 10. Wireless 802.11 tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Profile</td>
<td>Site profiles allows you to save and retrieve wireless parameters, rather than re-keying the parameters every time you change sites.</td>
</tr>
</tbody>
</table>
| Monitor Wireless Traffic by | Choose one of the following:  
Scan Channels—Click the **Channel Map** button and choose which channels you want to scan, then choose how often you want to scan them.  
Scan Interval—Define the scan interval.  
Fixed Channel—Pick a channel to monitor.  
BSSID—Specify the Basic Service Set ID of the Access Point you want to monitor.  
ESSID—Specify the Extended Service Set ID of the network you want to monitor. |
| Use encryption keys     | If your wireless network is secured, you must provide an encryption key for Observer to be able to capture and decrypt the wireless traffic. Select the Edit Encryption Keys button and provide your wireless encryption key. |
| Antenna to use          | The type of antenna connected to your system. Specify one of the following:  
Antenna Diversity—Use the stronger signal from the two antenna ports. This is the recommended setting for the standard snap-on antenna.  
Primary Antenna Only—If you are not using the standard snap on antenna, choose this option if the antenna you are using is connected to the primary antenna port (see your NIC manual for details).  
Secondary Antenna Only—If you are not using the standard snap on antenna, choose this option if the antenna you are using is connected to the secondary antenna port (see your NIC manual for details). |

Table 11. DS3/E3/HSSI tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Type</td>
<td>Choose DS3 (T3), E3 or HSSI to match the type of link you are analyzing, then choose the frame check sequence (FCS) standard: CRC-16 (the default) or CRC-32.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>You must set this to match the settings on the frame relay CSU/DSU.</td>
</tr>
<tr>
<td>Subprotocol</td>
<td>If ATM or LAPB is the selected encapsulation method, you must choose the sub-protocols on the link.</td>
</tr>
<tr>
<td>Fractionalized</td>
<td>Check if your link is configured for fractionalized operation. Fractionalized DS3 and E3 are not supported.</td>
</tr>
<tr>
<td>Bandwidth (HSSI)</td>
<td>Set to match the bandwidth and channel settings of the fractionalized HSSI link under analysis.</td>
</tr>
</tbody>
</table>

Table 12. T1/E1 tab

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN/Frame Relay Type</td>
<td>Choose T1 or E1 to match the type of link you are analyzing.</td>
</tr>
</tbody>
</table>
Understanding the Packet Broker Integration tab

When using network packet broker integration, you can dynamically reduce traffic flow to your GigaStor when it is at risk of oversubscription giving you the content you need. Additionally, metadata tags identify the network segment where the packets came from, providing you context when troubleshooting.

As a network administrator, you need really good content to be able to quickly troubleshoot your network environment. If you do not have the appropriate metadata or packets, determining where a problem is occurring and, more importantly, why the problem is occurring is very difficult. Content is king, and context is important. Dynamic traffic management gives you the content, and port tags give you the context.

Dynamic traffic management

Dropped packets are never desirable and they occur when a link is oversubscribed. If your analytics device does not have all of the packets of a conversation, troubleshooting is very difficult.

If your GigaStor is at risk of oversubscription, you should reduce the flow of traffic to the GigaStor. You have two options for reducing the traffic.

First, you can choose to pre-filter traffic using fixed, preset filters that you create. This is the minimalist approach. Second, you can allow all traffic and dynamically exclude traffic only when oversubscription occurs. We’ll explore each choice in a bit more detail.

With the minimalist approach to packet capture, you only capture the traffic that you think is relevant. In other words, you exclude everything from packet capture except the specific traffic you allow. For instance, you may decide that YouTube is not critical to your business and do not need to troubleshoot problems with that traffic. Therefore, you would never capture and save YouTube traffic. It is excluded with a pre-filter. This gives you longer retention capabilities for the content you do capture because your capture devices are not filling as quickly. Also, by not seeing YouTube and other non-critical traffic you are not overwhelmed with unnecessary information when troubleshooting. When you do identify a problem in your network, you can allow in more traffic by changing your pre-filters to troubleshoot the problem.

The opposite approach is to capture everything and use post-filters to find what you are looking for. If GigaStor is at risk of oversubscription, then using traffic
filters that GigaStor dynamically and automatically apply to a Gigamon can reduce the flow. This eliminates the oversubscription risk while continuing to capture the most amount of traffic relevant to you. You can set the types of traffic that interest you up front and GigaStor automatically captures it. After the initial configuration (page 42), it is no longer a manual process you need to remember to implement to capture the content you need. The dynamic filters allow you to focus on the business critical applications.

Figure 6: When filters are applied and removed

Unlike pre-filters, which can be used anytime, dynamic filtering is only available when using a Gigamon network packet broker.

**Contextual visibility**

Using Gigamon-applied port tags, you know which network segments are experiencing performance issues.

For context, you can have numerous streams of information coming into GigaStor, but, when you are troubleshooting, it is very helpful to know where in your network the packets came from. This is where port tags help. With port tags you have the context of knowing where in your network the problem occurred.

Figure 7: Contextual visibility
Using the port tags helps you solve correlative analysis issues. For example, if you are troubleshooting a VoIP call that shows excessive jitter or a low MOS score, it is important to know what portion of the network you are seeing in the packet captures. One network segment may not be experiencing any problems at all, while the other network segment does. By filtering on conversation and port tags, you will be able to see the conversation from different perspectives and begin to draw conclusions.

How to configure packet broker integration

Using a network packet broker ensures that the Observer Platform has the right content at the right times so that you can troubleshoot your network.

Configuring packet broker integration allows GigaStor to work with systems such as GigaVUE.

Using filters created in GigaStor, you can filter traffic as it leaves your packet broker reducing the load the GigaStor. Using Gigamon-applied port tags allows you to identify packets that come from your network packet brokers.

Prerequisite(s):

Exactly these versions are required:

- Gigamon Fabric Manager 3.3
- Gigamon GigaVUE H series nodes 4.6

With this feature, you can choose to use port tags without enabling dynamic filters, or you can decide to use dynamic filters and not use port tags, or you can enable both. You decide what is best for your environment.

You might choose to filter traffic because you only want certain traffic to be kept on this GigaStor or because the traffic load temporarily exceeds the GigaStor FIFO abilities. If there are multiple filters, they are applied one at a time in descending order until the FIFO level drops below 50%.

1. Select a probe instance in the Probes list.
2. Right-click and choose **Probe or Device Properties**.
3. Choose the **Packet Broker Integration** tab.
4. Use the information in **Packet Broker Integration (page 43)** to configure GigaStor to work with your packet broker.
GigaStor sends commands to your packet broker whenever FIFO levels are too high (above 50%). This temporarily reduces the traffic load coming into the GigaStor until FIFO levels drop below 20%.

**What to do next:** Turn on the NPB Port Tagging tab in GigaStor Control Panel in Setting the GigaStor general options.

**Packet Broker Integration**

Use the packet broker integration settings to configure the connection between GigaStor and your packet broker (for instance, GigaVUE).

<table>
<thead>
<tr>
<th>Fabric Manager address</th>
<th>The DNS name or IP address of the GigaVUE-FM system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster ID</td>
<td>The cluster name or IP address of the GigaVUE-FM visibility fabric node.</td>
</tr>
<tr>
<td>Username</td>
<td>Your GigaVUE-FM user name.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for your GigaVUE-FM user name.</td>
</tr>
<tr>
<td>Test Configuration</td>
<td>Use this button to validate your packet broker settings, including addresses, user name, and password. If you enter any invalid ports, a message box returns with a list of valid ports for the cluster.</td>
</tr>
<tr>
<td>Enable Gigamon port tagging</td>
<td>Provides contextual visibility by using the GigaVUE-FM-applied VLAN 802.1Q port tags that are added to every packet. This allows for filtering in GigaStor. Be sure to turn on NPB Port Tagging in Setting the GigaStor general options to show the NPB Port Tagging tab in GigaStor Control Panel where you can</td>
</tr>
</tbody>
</table>
see the GigaVUE-FM port from which the packet came, the port tag, the number of packets from the port, the amount of bytes, and utilization.

<table>
<thead>
<tr>
<th>Enable Dynamic Filtering</th>
<th>Allows the GigaStor to send filters to GigaVUE-FM whenever the FIFO load on the GigaStor reaches 50% and there is a risk of dropping packets. When this option is enabled, GigaStor clears any existing filters on Gigamon and replaces them with the new filters. When disabled, GigaStor removes all filters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool ports attached to this instance</td>
<td>A list of Fabric Manager ports that are associated with the GigaStor active instance. They are listed in the format required by Fabric Manager: Chassis/Slot/Port. For example, 1/1/x1.</td>
</tr>
<tr>
<td>Port (Chassis/Slot/Port)</td>
<td>The first value is the GigaVUE chassis in which the port is found, the second value is the slot within the GigaVUE chassis where the port is found, and finally is the port itself. All three values are required and must be separated by the / character.</td>
</tr>
<tr>
<td>Enable rollback of filters</td>
<td>If selected, any filters in the Applications to be filtered list that have been applied to the packet broker are removed after the specified number of minutes. The minimum is one minute. The time frame you choose allows for a smooth rollback of filters so that a momentary drop in network traffic does not cause filters to be repeatedly applied and removed in a short timespan.</td>
</tr>
</tbody>
</table>
| Applications to be filtered | This section defines the filters to push to GigaVUE to exclude certain content before the traffic is sent to GigaStor. Each time you add, remove, change, or reorder these filters, all filters on the GigaVUE system are deleted and replaced with these filters. This ensures that only the filters you specify in this list and no others are used.

The risk of dropping packets occurs when the FIFO reaches 50%. When that level is reached, a message is logged and the first filter in the list is applied. If applying the filter does not lower the FIFO level below 50% within one second, the next filter is applied. This process continues until the FIFO level remains below 50%. This ensures that a minimum number of filters is applied while allowing the most amount of traffic to be written to GigaStor.

The order of the filters is important. Filters are applied in descending order. In other words, the filter listed at the top is applied first, then the next if necessary, and so on. If the FIFO does not drop below 50% even after all filters have been applied, you should identify other application traffic to exclude. Filters are removed in reverse order starting with lowest priority (last) filter, then the next lowest, and so on until all filters are removed only after the GigaStor FIFO falls below 20% with that filter applied and the allotted time from the Enable rollback of filters field has passed. If the FIFO level goes back above 50% the filter that was just removed will be reapplied. The 50% and 20% threshold values are fixed and cannot be modified. Use the arrows buttons to change the order of your filters to find the arrangement that works best for you.

The buffer size of the active instance affects FIFO abilities. Changing the buffer size is described in Setting the GigaStor general options and may help in some instances; otherwise application filtering is needed.
You can choose to filter TCP-, UDP-, and SCTP-based applications, including any derived applications you created in How to add application definitions.

In GigaStor, an application can be defined using a port, port range, or port/IP address combination (or any combination of these). GigaVUE does not have a way to identify applications based on port/IP address. Therefore, the port/IP address combination will be removed from any filter before it is sent to GigaVUE. For example, if an application definition is 9000, 2343:10.74.33.101, only 9000 will be passed to GigaVUE; 2343:10.74.33.101 will be dropped from the filter. Again, this is a limitation of GigaVUE.

A maximum of 100 tool port filter rules can be created. An application that uses a port range (9001-9005) counts as one rule not as five rules.

GigaStor uses a REST API to communicate with GigaVUE. If there are communication interruptions between the two systems for whatever reason, GigaStor will attempt several times to reissue the command until it is successful. If it is still not successful after several attempts, a message will be written to the log.

How Gigamon-applied port tags are identified

GigaStor identifies packets with headers applied by Gigamon because a Gigamon system tags packets using an 802.1Q tag.

The Gigamon administrator may apply port tags to each ingress port on the GigaVUE. For each ingress port a unique VLAN 802.1Q tag is used. This tag is applied using the outermost VLAN tag. When there is a VLAN 802.1Q tag on the inner frame, only the information in the outermost 802.1Q tag is used.

GigaStor queries the list of port tags used by Gigamon and maintains a copy of that list. When traffic is received by GigaStor it is compared against the list. If there is a match, the GigaStor knows exactly which ingress port on the Gigamon was used and displays the information accordingly.

How to encrypt captured data at rest

Captured data at rest can be encrypted using the 256-bit Advanced Encryption Standard (AES) algorithm. This significantly increases the security of your at-rest data.

Prerequisite(s):

- You must have a special Observer license to enable and use this feature. There is no extra charge for the license.
- You must have a GigaStor hardware appliance. This feature is not available to GigaStor Software Edition. See the differences in software and hardware offerings for GigaStor.

Data at rest encryption is prevents visibility into any packets or even the metadata about the packets stored on the GigaStor. Any packets that are captured by the GigaStor are considered "data" and while they are stored on the GigaStor they are considered "at rest." Should any of the drives in the GigaStor be removed or misplaced, the data on the drives is protected. There is no remote access to this data apart from Observer's own analyzer, and the data tagging
methods for organizing and retrieving data can only be used in conjunction with Observer.

The GigaStor can capture 10 Gb line rate while simultaneously encrypting the traffic with AES-256 encryption without any significant performance impact on write or read speeds of the GigaStor. The RAID hardware is responsible for the encryption, and the data is encrypted before it is written to disk.

These instructions describe how to apply data at rest encryption to a GigaStor already in your possession. If your GigaStor shipped from the warehouse with the data at rest security already enabled, you do not need to complete this process unless two or more drives in your RAID have failed.

Caution: This procedure deletes all of the data on your GigaStor! Ensure you have a backup of any data you wish to keep.

1. Download the latest firmware for the Areca 1882 Series RAID card or contact VIAVI Support for the file.

2. Choose Start > All Programs > Areca Technology Corp > ArcHttpSrvGui > Areca HTTP Proxy Server GUI. The program starts. You should see something similar to the Figure 9 (page 46) image.

3. Select Controller#01 and click Launch Browser. If the controller is not running, click the Start button then launch the browser. The Areca RAID application attempts to connect to its web server.

4. Type the user name and password. The default user name is admin. There is no default password. Click OK to open the browser.

In the browser you can see the RAID set, IDE channels, Volume, and capacity.

5. In the web browser, choose System Controls > Upgrade Firmware. In the Browse field, choose each of the four files from the firmware package you downloaded or received from Technical Support in step 1 and click Submit. Choose the files in the order they are listed below. After adding the arch1882fim.bin file you are prompted to restart the system. Ignore that restart request and add the fourth file.
6. Restart the GigaStor.

7. Choose **Volume Set Functions > Delete Volume Set**. Select the volume, then select **Confirm The Operation** and click **Submit**. This deletes all of the existing data on the RAID.

8. Choose **Volume Set Functions > Create Volume Set**. Set the following options to these values, select **Confirm The Operation**, and click **Submit**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume RAID Level</td>
<td>Raid 5</td>
</tr>
<tr>
<td>Greater Two TB</td>
<td>64bit LBA</td>
</tr>
<tr>
<td>Volume Support</td>
<td></td>
</tr>
<tr>
<td>Volume Initialization Mode</td>
<td>Foreground Initialization. It may take several hours (six hours for 48 TB) to initialization the volume. While the volume is being initialized, the GigaStor cannot be used. If you choose Background Initialization, you may use your GigaStor, but it will take significantly longer to complete and performance will be negatively affected.</td>
</tr>
<tr>
<td>Volume Stripe Size</td>
<td>128</td>
</tr>
<tr>
<td>Volume Cache Mode</td>
<td>Write Back</td>
</tr>
<tr>
<td>Volume Write Protection</td>
<td>Disabled</td>
</tr>
<tr>
<td>Full Volume Encryption</td>
<td>256Bit Key, AES Key</td>
</tr>
<tr>
<td>Tagged Command Queueing</td>
<td>Enabled</td>
</tr>
<tr>
<td>SCSI Channel</td>
<td>0:0:0</td>
</tr>
<tr>
<td>Volumes To Be Created</td>
<td>1</td>
</tr>
</tbody>
</table>


   Because this is the first time that Observer is opened with the new license, it does not yet have a key for the encrypted volume. A window appears indicating that the volume is locked.

10. Click **Generate Key** and save the key file in a secure location following your organization’s security policy.

   - When rebooting, the system needs access to key in order to unlock the drive. This is the key necessary to write to and read from the RAID volume.
   - Observer will not open unless it can find the key. Without the key present neither packet capture nor packet analysis can occur. You can choose to remember the key file location so that Observer opens automatically, or, if left cleared, each time Observer is opened you must provide the path to the key file.
   - Securely storing the key is a critical part of your responsibility.

11. Close Observer until the rest of this procedure is complete.
12. In Control Panel > Administrative Tools > Computer Management > Storage > Disk Management select the RAID volume, right-click and choose Initialize. In the Initialize Disk window, select Disk 1 and GPT (GUID Partition Table). Convert the volume to a Simple Layout, assign a drive letter (typically, D:), and provide a name (typically, DATA).

13. Repeat this process for each RAID volume for your GigaStor.

14. Open Observer.

**Using the Probe**

The probe has two interfaces: the probe service and the analyzer user interfaces. You can switch between the two depending on what you want to accomplish. Also learn about monitoring a wireless access point (AP) and where to enable network trending.

**Using the Expert Probe software**

Learn how to create, configure, redirect, and delete both local and remote probe instances.

**Prerequisite:** Expert Probe

The Expert Probe is a step above the Multi Probe software and is the only probe software that runs on the GigaStor. The Expert Probe includes all the functionality of the Multi Probe, plus it displays remote expert analysis in real time for faster troubleshooting. If you are using the Expert Probe on a GigaStor (rather than a non-GigaStor probe) there are even more features available. Just like the Multi Probe, the Expert Probe has a number of tabs that allow you to control probe network connections and memory usage, administer probe security, and monitor probe activity.

**Figure 10: Expert Probe on a GigaStor**

An Expert Probe transfers decode data to an Observer only when you select the packet from the one-line summary pane, which is updated with packet header information in real time. This conserves network bandwidth by analyzing all data locally and sending only the results. This eliminates the need to transfer data packets over the wire. This differs from the Single Probe and Multi Probe because those probes send the entire buffer to the analyzer and the decoding and analysis happens on the analyzer.

Another feature exclusive to the Expert Probe is its ability to switch between being a probe or an analyzer. This can be very useful depending on your needs. This gives you flexibility in using the probe both remotely and on site.
VoIP Expert, Application Performance Analysis, and Application Transaction Analysis

**Prerequisite:** Expert Probe

The Expert Probe provides unique insight into your OSI Model Layer 7 applications that the Multi Probe and Single Probe cannot provide. This is especially true for VoIP.

There is nothing that you need to configure on the probe to enable these features, but this information is only available when viewing the probe instance of an Expert Probe.

To use and configure VoIP, ATA, or APA:

2. Use the General, Application Transaction Analysis, Application Performance Analysis, and VoIP tab to configure your options.

3. Click the **Start** button to begin monitoring.

4. After you have collected some data, click the **Analysis** button. The View Network Trending data dialog opens.

5. Choose “Transfer and view current day statistics” and click **OK**. This opens the Network Trending Viewer in a new tab where you can see your data.

Switching between the probe and analyzer user interfaces

Most probes can be run as either a Windows service or in application mode. Some settings can only be made when the probe is in application mode.

**Prerequisite:** Multi or Expert Probe.

Depending on how you want or need to use your Expert Probe, it can be either an Observer to help you view your network data or it can be a probe to capture data and to which other Observer can connect. The Expert Probe software cannot simultaneously be an analyzer and a probe.

To change the Expert Probe interface to load as a fully-featured Observer, click **File** and . You must restart the application to see the change.

**Note:** For a GigaStor, the Expert Probe software is running as a Windows service. You must stop the Expert Probe service before you can change its interface.

1. Right-click the **Probe Service Configuration Applet** in the system tray and choose **Open Probe Configuration**.

   Figure 11: Probe Service Configuration Applet

   The **Probe Administration** window opens.

2. Choose **Options > Probe Options**.

3. Clear the option **Run Probe as a Windows Service** option, and click **OK**.

   This removes the VIAVI Expert Probe service from Windows.
4. Start Observer.
6. Choose Observer, click OK, and click OK again when prompted.
   This closes Observer.
7. Start Observer.

Observer is now set to use the analyzer interface.

When switching back to an Expert Probe on the GigaStor, you must reverse these steps and then you must manually start Expert Probe from the Windows Service Control Manager. It may take a moment before the service starts. You may need to restart the GigaStor for the setting changes to fully set.

Enabling Network Trending and setting which statistics are collected

A probe can provide many different statistics about your network, but you must enable the collection of those statistics. Network Trending does not capture packets, but collects statistics about the traffic on your network. Many reports in Observer use the trending information, and we recommend you enable Network Trending.

1. To turn on the collection of a specific statistic, in Observer choose Statistics > and then select the statistic you want to have the probe collect and report.

Monitoring a wireless access point

You can capture all wireless traffic with a wireless network card on a laptop or any system with a wireless network card if you use the VIAVI wireless driver. The default driver for your wireless card is not sufficient for Observer.

Standard network cards do not support “raw” wireless packets, nor do they enable “promiscuous” mode by default. Promiscuous mode captures all packets for the analyzer, not just those addressed to the network card. Both “raw” wireless packets and promiscuous mode are required by Observer. The VIAVI wireless driver enables these options.

When a network card is running in promiscuous mode, it cannot connect to a wireless access point. It can only capture traffic. If you are using a laptop and want to capture traffic and at the same time connect to a wireless access point, your laptop must have two wireless cards.

If you are using the probe software on your laptop, you need two network adapters. Typically, one adapter is an Ethernet card for communication and one wireless adapter for analysis. You could also use two wireless cards. You may also need special drivers.

If your wireless network uses an encryption key or specific wireless channels, you can specify that information for the wireless adapter.

Note: use private keys to authenticate with a RADIUS server, then dynamic keys are used to encrypt communication on a user by user basis, with no two users ending up with the same keys. Observer cannot decrypt the data from a site that implemented EAP/LEAP, but this does not mean Observer is not useful. Because all management and control packets are not encrypted, wireless troubleshooting is not affected even if you use EAP/LEAP. If you want to troubleshoot the actual data in the conversation, collect the data
Using the probe as a virtual TAP

Learn when to use a virtual TAP, its purpose an benefits, and how to configure them for use in a VMware ESX server.

**Prerequisite:** Multi or Expert Probe.

The Virtual TAP (sometimes called a vTAP) allows you to configure a virtual tap to monitor traffic within a virtual host environment.

Most virtual environments provide virtual adapters for each virtual machine, and these virtual adapters are logically connected to a virtual switch managed by the virtual host system. The virtual switch manages traffic flow to and from the virtual adapters by mapping each virtual adapter to a physical adapter in the host. When promiscuous mode is enabled on a virtual adapter (or virtual switch), all traffic flowing through the virtual switch—including local traffic between virtual machines and remote traffic from outside the virtual host—is sent to the promiscuous virtual adapter and can be monitored by Observer.

To use the virtual tap you must monitor all virtual machines in a host from a virtual machine within the host. This assumes you can use a SPAN/mirror port or the virtual NIC has a "promiscuous mode" setting. This functionality is available in VMware's ESX and ESXi. It may also be available in other virtual server products.

Using the virtual TAP, you can then collect and re-direct all traffic internal to the virtual switch to a dedicated virtual NIC within the monitoring virtual machine that is then connected to Observer.

If there is any internal communication between virtual machines, the only way to monitor this data is by using a separate monitoring virtual machine with an analysis service (for instance, probe) gathering data from the internal virtual switch. Should you need to analyze or store data on a GigaStor, installing a Virtual TAP within the monitoring virtual machine provides complete visibility into all data flowing on the internal virtual switch.

You can create a port group on a switch and use a virtual machine (VM1) to monitor traffic of a second virtual machine (VM2) that resides on the same switch but in different port.

**Tip!** If you already have a 64-bit Windows virtual machine, we suggest you use it, because installing the probe there will be less resource intensive on the host than installing a new virtual machine on the host.

1. Do one of the following:
   - On the probe: Click the Virtual TAP tab.
   - In Observer: Select a probe instance, right-click and choose Administer Selected Probe. Then click the Virtual TAP tab.
2. Click Modify to set the source and destination adapters for the virtual tap.
3. Choose your source and destination adapters and select the Enable Virtual Tap option.

You have now configured what you need to within Observer to enable the virtual tap feature, but you must modify a setting for your virtual switch.

4. Set the virtual NIC on the virtual switch within the host in SPAN/mirror mode, sometimes also called promiscuous mode. See your virtual machine’s documentation for further details.

When to use a virtual TAP

Monitoring network and application traffic in a virtualized environment containing one-to-many relationships between physical hardware devices (virtual hosts) and virtual application servers (virtual machines) presents a number of concerns.

Virtual environments are designed to include a virtual adapter (vNIC) for each virtual machine within the system. The vNIC is logically connected to a virtual switch, which is managed by the virtual host system (see the diagram below). This addresses communication which would remain in the VM host. In order to enable communication into and out of the VM host, a logical connection between the vNIC and the pNIC must be established.

Depending on the virtual server technology you have decided to implement, you have a number of options for network and application traffic visibility, and for the use of external devices for analysis. If all virtual machine communications take place between the virtual machines and the “outside” (i.e., outside the physical host), then monitoring the data flow from outside the host server may be the least complicated method by which to gain flow visibility. If there is any internal communication between virtual machines, the only way to monitor this data is by using a monitoring virtual machine (separate or existing) with an analysis service (i.e., probe) gathering data from the internal virtual switch. Should you need to analyze or store data on an external purpose-built device, installing a virtual TAP within the monitoring virtual machine provides complete visibility into all data flowing on the internal virtual switch.

Within the VMware ESX and ESXi environments, a virtual adapter can be set in “promiscuous mode.” When promiscuous mode is enabled on a virtual adapter, all traffic flowing through the virtual switch—including local traffic between virtual
machines and remote traffic originating from outside the virtual host—is sent to the promiscuous virtual adapter.

A number of challenges are presented when attempting to monitor applications with a virtualized environment.

1. **Lack of visibility.** Traffic between virtual machines within a virtual host will not be visible outside of the host. This causes a number of problems:
   a. Network engineers cannot monitor multi-tier applications partially or wholly located on multiple virtual machines within a single host.
   b. Should a virtual machine be compromised by malicious code or security breach, other virtual machines within the same host may also be compromised.

2. **Lack of analysis functionality.** A separate solution is required to push data streams flowing within virtual machines out to an external tool or a purpose-built device. This functionality is necessary for network and application monitoring and analysis, compliance, and security audits. Virtual TAPs (software applications placed inside a virtual machine to export all data through a designated pNIC to an external device) can alleviate this problem.

**Options**

The goal is to not only see all traffic flowing within a VM host but also export that data for powerful analytics and reporting. There are three primary ways to monitor both traffic flow from within applications on virtual machines and from the virtual host.

1. Monitor the host using an external analysis device as you would any other system, via SPAN technology or a physical TAP. This option works well for environments not needing to track internal virtual machine-to-machine traffic.
Within a host. However, it may not catch a security breach compromising multiple virtual machines within a host.

2. Monitor all virtual machines in a host by establishing a new virtual machine within the host. This option assumes the ability to SPAN or set in promiscuous mode the virtual switch within the host. This option provides visibility at the statistics and packet levels of all traffic within a virtual host. It does not,
however, allow packet-level traffic to be analyzed by an external physical device (IDS, retrospective analysis device, etc.).

3. Use a virtual TAP to collect and redirect all internal virtual machine traffic to a dedicated virtual NIC within the monitoring virtual machine that is connected to an external purpose-built device for analysis or compliance enforcement. Depending on the functionality of the external device the traffic is being copied to, this option may provide all the functionality of option two while
taking advantage of the physical capabilities of the purpose-built external device.

Option two combined with option three offers the most extensive and comprehensive monitoring solution. In a VMware environment, you can use promiscuous mode on the internal virtual switch and direct a copy of all traffic from all virtual machines to a virtual machine monitoring instance. This allows you to collect metrics and perform real-time analysis; and using a virtual TAP, you can re-direct packet streams out a separate NIC to a GigaStor probe.

Benefits of a virtual TAP

Mirroring all traffic within a virtual host to an external device provides a number of advantages, including total visibility into VM application traffic and the ability to run greater analytics for comprehensive reporting and faster problem resolution.

For example:

- **Application Performance Monitoring.** Feed VM traffic to an enterprise reporting engine for comprehensive monitoring of virtualized environments. Set and track performance baselines and respond quickly when performance deviates from the norm. Tracking VM traffic over time helps determine if your VM server load has increased to the point of requiring action.

- **Application Performance Troubleshooting.** The virtual TAP can also output data to a GigaStor probe, which stores it for later access. The GigaStor can help isolate problems within your virtual environment and troubleshoot these issues using Application Analytics.

The Virtual TAP option bridges the visibility gap, allowing complete real-time analysis, Retrospective Network Analysis, and full-scale reporting on all virtualized traffic.
Configuring VMware ESX Server

A virtual machine is a convenient way to add monitoring capabilities to your network. Use this information to create a virtual switch.

**Prerequisite(s):**
- Your virtual machine meets the [minimum specifications (page 15)](#)
- Multi or Expert Probe is installed
- A free physical NIC

The default policy for Promiscuous Mode for the vSwitch itself should remain in the Reject setting. Only the new port group within the vSwitch should be set to Accept Promiscuous mode. You can use the virtual machine properties dialog to identify the Network Connection, listed in the Windows Network Connections dialog, by unchecking the "connected" option.

In the virtual switch to be monitored, add a virtual port group and set it to run in Promiscuous Mode.

**Caution:** Do not choose the same source and destination for the Virtual TAP Settings. This could cause broadcast/multicast loops and would noticeably impact your network.

1. Open VI Client and highlight the VMware ESX Server Entry.
2. Click the **Configuration** tab.
3. Click **Hardware – Choose Networking**.
4. Find the vSwitch for which you would like to monitor traffic and choose Properties.
5. In the vSwitch Properties dialog (Ports tab), click **Add**.
6. In the Add Network wizard, choose Virtual Machine [port group], give the group a name (“Promiscuous Port Group”), and finish the wizard.
7. In the **vSwitch Properties** dialog, highlight the new port group and click **Edit**.
8. Click the **Security tab**.
9. Select the **Promiscuous Mode Policy Exception** option and change the list to Accept.
10. Setup a second virtual switch and bind a second physical NIC to that virtual switch.

See Figure 13 (page 58) Virtual Infrastructure Client > Configuration tab. Then see Figure 15 (page 59) Add Networking > Add Network Wizard > Virtual Machine.

11. Create a virtual switch.

12. Select the appropriate NIC entry (i.e. Physical NIC 2 on ESX Server).

13. Name the vSwitch (i.e. “vTAP OUT to GigaStor”) and finish.

The result should be similar to Figure 14 (page 59). See your VMware ESX Server documentation if you need more detailed information on adding a virtual switch.
14. Edit the Virtual Machine that contains the Observer to use the Port Monitor Group and second vSwitch.
15. Select the first network adapter.
16. Change the Network label to the new Port Monitor Group, and add a second virtual NIC if needed.
17. Select the second virtual NIC and change the Network label to the second vSwitch (i.e., vTAP OUT to GigaStor) and click **OK**.
18. Verify that the Virtual Machine containing Observer is located in both virtual switches.

**Figure 15: Virtual Machine Properties**

19. Within the virtual machine, setup Observer to VTAP Local Area Connection 1 to Local Area Connection 2.
20. Connect the cable from “NIC 2” on the VMware ESX Server to the GigaStor capture card.

**How to assign physical ports to probe instances**

By default, the active instance monitors network traffic from every physical port of your capture card—all the traffic is aggregated. If you want to instead “divide” your monitored network traffic by physical ports, to help you monitor certain SFPs separately from others, then you can use virtual adapters to assign specific physical ports to probe instances.
Prerequisite(s):
Your hardware appliance must have one of the following:
- Gen2 capture card
- Gen3 capture card

For example, suppose you are deploying an 8-port Gen3 capture card as follows:
- Ports 1-4 are monitoring a collection of trunked links
- The remaining ports are each connected to the SPAN (or mirror) port on a switch

In this scenario, it makes sense for Observer to view ports 1-4, for example, as a single stream of network traffic and to separate each of the four remaining ports into separate data streams. Virtual adapters are a convenient way to accomplish this separation or aggregation in real time, rather than depending on filters to sort through the traffic post-capture.

These are the general steps for assigning physical ports to a probe instance:
- Create a virtual adapter (or have one already).
- Assign physical ports to this virtual adapter.
- Set a probe instance to use this virtual adapter as its NIC.

Tip! As a general reminder, you risk severe performance loss when using more than one active instance. These instructions do not create multiple active instances.

To assign physical ports to a specific probe instance:
1. In Observer, right-click the Gen3 capture card-equipped probe instance from the probe list, and click **Probe or Device Properties**.
   A Gen3 capture card-equipped probe instance shows (Gigabit) or similar after the name.
2. Click the **Virtual Adapters** tab.
3. Select a virtual adapter, and click **Edit Adapter**.
4. Select physical ports from the **Available Ports** list, and click **Add**.
   You can select more than one physical port by holding **CTRL** as you click.
5. Click **OK** to return to the **Virtual Adapters** window.
6. Click **OK** to save the virtual adapter and close the **Virtual Adapters** window.
   Changes to virtual adapters are not be saved until **OK** is clicked in the **Virtual Adapters** window.

The virtual adapter appears in the list of available network adapters when creating a probe instance. This allows you to assign the virtual adapter to a specific probe instance, among other benefits.
Next, you should change the monitored network adapter (page 27) of a probe instance to use the virtual adapter.

**Using the NetFlow features in Observer**

Watch a video about NetFlow in Observer, and see a list of some important NetFlow considerations to know.

Like many things in Observer a feature is not in just one place, but spread throughout the product. NetFlow is no different. Use this section as a starting place to find what you need regarding NetFlow in Observer.

- Choose the right probe for you.
- Ensure your ToS/QoS is set for your network so that your statistics are correct.
- There are two different types of NetFlow collectors. Learn the differences and see how to create one.
- Capturing NetFlow statistics does have some limitations that are different from packet capture.
- Decoding a NetFlow flow. This section also details how you may need to configure your NetFlow device so that Observer can see the flows.
- Open a saved NetFlow capture.
- Most NetFlow information comes from Network Trending.

**Creating a NetFlow collector or NetFlow Trending collector**

There are two types of NetFlow collectors in Observer. Choose the correct one for your needs, or create two different probe instances—one for the NetFlow collector and another for the NetFlow Trending collector.

**Prerequisite:** Expert Probe

| Note: | If you want to have scheduled collection of your NetFlow devices, use the settings on the Schedule tab. |

NetFlow and sFlow collectors support the following versions of these technologies:

- NetFlow: 1, 5, 7, 9, and 10 (IPFIX)
- sFlow: 2, 4, and 5

There are two types of NetFlow collectors in Observer. Choose the correct one for your needs, or create two different probe instances—one for the NetFlow collector and another for the NetFlow Trending collector. In most cases, it will likely be the NetFlow Trending collector. The NetFlow Trending collector supports up to 50 NetFlow devices, whereas the NetFlow collector only supports one NetFlow device. That means you must add and configure a NetFlow collector for each NetFlow device in your environment.
### NetFlow Trending Collector vs NetFlow Collector

<table>
<thead>
<tr>
<th>Feature</th>
<th>NetFlow Trending Collector</th>
<th>NetFlow Collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>One flow per collector</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Up to 50 flows per trending collector</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Collects live statistics(^1)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Collects historical trending(^2)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

1. Live statistics are details about the flow that appear in Observer in as few as five seconds.
2. Historical trending data collection interval can be as few as 60 seconds.

See [Creating a probe instance (page 24)](#) for details about creating a NetFlow collector or a NetFlow Trending collector. In [Creating a probe instance (page 24)](#) choose NetFlow collector or NetFlow Trending collector and follow the on-screen instructions. After the probe instance is created, there is no other configuration you must do and it is ready to use.

After the probe instance is created, you may want to configure the probe to tell it what type of traffic is seen.

2. On the General tab, configure the Timing and Statistics Packet Sampling sections for your needs and [Click OK](#).

4. [Click the Settings button](#).

5. Configure any settings for Network Trending here.

6. [Click OK](#) to close the Network Trending Settings window.

7. [Click the Start button](#) to begin monitoring the NetFlow devices.

8. After you have collected some data, [click the Analysis button](#). The View Network Trending data dialog opens.

9. Choose “Transfer and view current day statistics” and [click OK](#). This opens the Network Trending Viewer in a new tab. In the Network Trending Viewer you can see for your NetFlow devices:
   - Station Activity Time
   - Top Talkers
   - Packet Size Distribution
   - Bandwidth Utilization
   - Protocols
Chapter 3: Understanding How a Probe Uses RAM

How a probe uses RAM

A Windows computer uses Random Access Memory (RAM) as a form of temporary data storage. Windows separates all available memory into three sections: protected memory, user memory, and reserved memory. An Observer probe, depending on how it is configured, uses these types of memory differently.

The protected memory is used to load critical operating system files, such as device drivers. If any of this RAM is dedicated to a driver or some other critical file, it cannot be used by another program. However, after Windows finishes loading its drivers, the memory is freed and any program may access the remaining protected memory.

User memory is all available memory beyond the protected memory. It is available to any application at any time. The probe uses this memory to temporarily store statistical information, such as Top Talkers data.

Reserved memory is user memory that you have specifically set aside for use by the Observer probe. Only the probe may use that portion of RAM. When the RAM is reserved for the probe not even the operating system may access it—even when Observer is closed.

By having RAM reserved specifically for the Observer probe, you ensure that the probe has the memory necessary to capture packets and store these packets for statistical processing. If Observer runs without any reserved memory, it requests and uses the operating system's protected memory for capturing packets. There is no adverse effect of running an Observer probe without reserved memory, but it is not the most efficient way to run the probe. By default, the probe uses no reserved memory. Our recommendation is that you reserve memory for Observer
so that the probe runs efficiently and leaves the protected memory for the operating system and other programs to use.

Packet captures are always written sequentially from the first open byte of RAM in reserved memory or in Windows protected memory. They are written until all available space is used. If you are using a circular buffer, then the first packet is overwritten with the newest packet. This is first-in, first out (FIFO). With Windows protected memory, your capture space is limited to about 50 to 80 MB, but with reserved memory you have the potential to store many gigabytes in memory. Figure 17 (page 65) describes the two different ways that Observer runs.

Figure 17: Windows protected memory, user memory, and reserved memory

Whether using protected memory or reserved memory, Observer uses the RAM to store data for things such as (and creates a section within the RAM dedicated to):

- Packet capture
- Statistics queue buffer
- Collected statistical memory

Network packets seen by Observer are passed to both the packet capture memory and to the statistics queue buffer. After a packet is processed by the statistics queue buffer, the statistical information is passed to the statistical memory. All packets in both the packet capture memory and the statistical queue buffer stay in memory until the buffer is full and the oldest packets are replaced by newer packets (using FIFO).

Figure 18 (page 66) shows what options in Observer control the size of various portions of memory.
Packet capture buffer and statistics buffer

There are two kinds of buffers that a probe uses to store data in real-time: capture buffers and statistical buffers. The capture buffer stores the raw data captured from the network while the statistical buffer stores data entries that are snapshots of a given statistical data point.

Selecting an appropriate capture buffer size given system resources is all most users need to worry about; the default settings for the statistical buffers work perfectly fine in the vast majority of circumstances.

However, if you are pushing the limits of your probe system by creating many probe instances, you may be able to avoid some performance problems by fine-tuning the memory allocation for each probe instance.

For example, suppose you want to give a number of remote administrators access to Top Talkers data from a given probe. You will be able to add more probe instances within a given system’s memory constraints if you set up the statistics buffers to only allocate memory for tracking Top Talkers and to not allocate memory for statistics that no one will be looking at.

Observer has no limitations on the amount of RAM that can be used for a buffer. Note that when run on a 64-bit Windows, there is no 4 GB limitation for the capture buffer; you are limited only by the amount of physical memory installed on the probe.

In all cases, the actual buffer size (Max Buffer Size) is also reduced by 7% for memory management purposes. Should you try and exceed the Max Buffer Size an error dialog will be displayed indicating the minimum and maximum buffer size for your Observer (or probe) buffer.

For passive probe instances, which are most often used for troubleshooting, the default settings should be sufficient. If you are creating an active probe instance (one that writes to disk and not just reads from it), then you may want to use the following formula as a rough guideline to determine how much RAM to reserve.
for the probe instance when doing a packet capture. (This formula does not apply when doing a Observer GigaStor capture to disk. It is only for probe instances doing packet captures.)

Use this formula to determine your RAM buffer size:

\[
\text{Network Speed} \times \frac{\text{Average Throughput (MB/second)}}{\text{Seconds of data storable in RAM}}
\]

**Tip!** You want a buffer that will handle your largest, worst case unfiltered burst.

Use this formula to determine how much hard drive space a capture requires (in GB) and Observer’s write-to-disk capability. There is no limitation to the amount data Observer can write to disk other than the disk size itself.

\[
\frac{\text{(Traffic Level / 8 bit)} \times 3600 \text{ Seconds}}{1024 \text{ bytes}} \text{ Gigabytes per hour}
\]

For instance a fully utilized 1 Gb port (1 Gbps is 125 MBps):

\[
\frac{(125 \text{ MBps / 8 bit)} \times 3600 \text{ Seconds}}{1024 \text{ bytes}} \approx 54.93 \text{ GB per hour}
\]

**Running Observer without reserved memory**

Single probes cannot use reserved memory. By default, no memory is reserved for Observer if you install it on your own system.

**Prerequisite(s):**

- All versions of Observer Expert, Observer Suite, Expert Probe software, and Multi Probe software installed on your own hardware, unless modified.
- Single Probe software at all times
- NetFlow probes

Observer without reserved memory is the default, but not recommended, configuration. It is the default because each network is unique and you must determine how you want Observer to be configured for your system.

**Note:** This section does not apply to the GigaStor or other hardware products from VIAVI. They are properly configured at the factory.

**Tip!** If you need more RAM for the statistics queue buffer, you may need to lower the amount of RAM dedicated to packet capture so that it is freed and available to add to the statistics queue.

After you install Observer and first open the program it does not have any reserved memory. Observer allocated a portion of the available protected memory for its use. This creates a “Windows memory pool” for Observer of about 50 to 80 MB (depending on the amount available from Windows, and cannot be increased). This is a limitation of the Windows memory pool and the Windows operating system.
Single Probes, unlike Multi-Probes and Expert Probes, cannot use reserved memory because of their design. By default, 16 megabytes is available for the Packet Capture and Statistics Queue buffer. Single Probes have a maximum of 52 megabytes that can be assigned from the Windows memory pool. Because of the Windows memory pool constraint, Single Probes are limited to a Packet capture buffer maximum of 72 megabytes, assuming you set the Statistics queue buffer to its minimum (12 megabytes). The Statistics queue buffer maximum is 76 megabytes if the Packet capture buffer is set to 0 megabytes.

1. Click the **Memory Management tab** to display the list of probe instances and their buffer sizes.

2. Click the **Configure Memory** button at the top of the window to view and modify how Observer uses the protected memory for this probe instance. The Edit Probe Instance window opens.

On the Edit Probe Instance window, you can see how memory is allocated for:

- Packet capture
- Statistics queue buffer

You can also see how much protected memory is still available in the Windows memory pool.

**Figure 19: Edit Probe Instance**

3. Use the arrows to the right of the Packet capture and Statistics queue buffer to increase or decrease the amount of RAM you want dedicated to each. See How to allocate the reserved RAM (page 72) to help determine how to divide the memory.
Running Observer with reserved memory

Reserved memory helps Observer run more efficiently by dedicating memory for its exclusive use.

**Prerequisite(s):**
- Observer Expert
- Observer Suite
- Expert Probe software
- Multi Probe software

Observer uses reserved memory for packet capture and the statistics queue buffer. It is highly-recommended that you use reserved memory. (GigaStor appliances running Observer are preconfigured this way.) You must determine how you want Observer to be configured for your system.

**Caution:** Never change the reserved memory settings of VIAVI hardware unless VIAVI instructs you do so. Reserved memory settings should only be modified on non-VIAVI hardware, such as a desktop computer running Observer.

**Tip!** If you need more RAM for the statistics queue buffer, you may need to lower the amount of RAM dedicated to packet capture so that it is freed and available to add to the statistics queue.

Reserving memory allows Observer to allocate RAM for its exclusive use. This ensures that Observer has the necessary memory to store packets for statistical analysis, or for capturing large amounts of data for decoding. The more memory you reserve for Observer, the larger the packet capture and statistical queue buffers can be.

If the memory buffer for the statistics queue buffer is too small, you may end up with inaccurate statistical data because some data may get pushed out before it can be processed. Observer processes packets on a first-in, first out (FIFO) basis, so it is important that the buffer be large enough to allow for processing.

When reserving RAM for Observer you are taking RAM away from the operating system. Table 13 (page 69) shows how much memory is required by the operating system. Anything beyond this amount may be reserved for Observer.

**Table 13. Reserved memory requirements**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>RAM required for the operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit with less than 4 GB RAM</td>
<td>800 MB</td>
</tr>
<tr>
<td>64-bit with 4 GB RAM</td>
<td>4 GB ¹</td>
</tr>
<tr>
<td>64-bit with 6+ GB RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>32-bit</td>
<td>256 MB (although 400+ MB is recommended)</td>
</tr>
</tbody>
</table>

1. Because of how 64-bit Windows loads its drivers when 4 GB of RAM is installed all 4 GB is used by Windows. This is sometimes referred to as the BIOS memory hole and means you cannot reserve
any memory for Observer. To capture packets on 64-bit Windows install either more than or less than 4 GB of RAM.
2. 32-bit operating systems do not support more than 4 GB of RAM. Observer cannot use any RAM above 4 GB.

1. To see how much protected memory the probe has, click the **Memory Management** tab.
2. Click the **Configure Memory** button at the top of the window to view and modify how Observer uses the protected memory for this probe instance. The Edit Probe Instance window opens.

On the Edit Probe Instance window, you can see how memory is allocated for:
- Packet capture
- Statistics queue buffer

You can also see how much protected memory is still available in the Windows memory pool.

3. Use the arrows to the right of the Packet capture and Statistics queue buffer to increase or decrease the amount of RAM you want dedicated to each. See How to allocate the reserved RAM (page 72) to help determine how to divide the memory.

4. After reserving memory for Observer you must restart the system for the changes to take affect. After you restart the system you can allocate the memory to the different probe instances.

**How packet capture affects RAM**

When you start a packet capture (Capture > Packet Capture and click **Start**), all packets that Observer sees are placed into the packet capture buffer (a specific portion of the protected memory). The packets stay in this protected memory until the buffer is cleared. If you are using a circular packet buffer, new packets overwrite old ones after the buffer is full.

**Figure 20 (page 71)** shows how Observer receives a packet and distributes it throughout RAM, and how it is written to disk for packet capture and GigaStor capture.

Packets received by the network card are passed to Observer, where Observer puts each packet into RAM, specifically in the packet capture memory buffer and the statistical queue buffer. If a packet must be written to disk for either a GigaStor capture or a Packet Capture, it is copied from the RAM and written to the disk.
Figure 20: How packets move through Observer's memory

- The capture card receives data off the network.
- The capture card passes data into RAM. In the RAM it goes into the packet capture buffer and the statistics queue buffer.
- The statistics queue buffer passes the information to the statistics memory configuration.
- The statistics memory configuration passes the data to the real-time graphs.
- The Network Trending Files receive data from the statistics queue buffer through the NI trending service, where they are written to disk.

The following steps occur only if you are writing the data to disk through a packet capture to disk or a GigaStor capture.

If you are using packet capture to disk, the packet capture buffer passes the data to the operating system's disk.

If you are using GigaStor capture, the statistics queue buffer and the packet capture buffer passes the information to the RAID.

A few notes about how some buffers are used:

- Packets received by the statistics queue buffer are processed and put in the collected statistics buffer.
- Data for network trending comes from the statistics queue buffer, then it is written to disk, and finally flushed from the buffer every collection period.
- The collected statistical buffer does not use first-in, first-out to determine statistics. Therefore, after the statistic limit is reached the remaining data is no longer counted; however, data for known stations continue to be updated indefinitely.
- Regardless of whether Observer is using reserved memory, the statistics memory, statistics queue buffer, and packet capture buffer function the same. The storage space available for storing packets in memory increases though when you reserve memory.
How to allocate the reserved RAM

After you have the RAM reserved for Observer, you must allocate it for the probe instances. Here are our basic recommendations for allocating the memory. These are just recommendations and may be changed or modified for your circumstances.

If you are using a GigaStor hardware appliance, read this section, but also be sure to consider the information in Recommendations for the VIAVI capture cards (page 72).

How many probe instances will you have on this system? How are you using the probe instance(s)? Are you using it to capture packets or to analyze statistics? After you know how you want to use the probe instance, you can decide how to properly divide the memory amongst the probe instances, and further how you will allocate the memory between the packet capture and statistics queue buffers.

You want to create and use as few probe instances as absolutely necessary. Each probe instance you create divides the memory pool into smaller chunks. The more probe instances you have, the more processing the system must do.

Note: If you have a lot of network traffic, then you may need to allocate at least one gigabyte of RAM to the packet capture buffer, the statistics queue buffer, or both.

For each probe instance determine:

- If you want to mostly capture packets, then allocate 90% of the reserved RAM to packet capture and 10% to the statistics queue buffer. At a minimum, you should allocate 12 MB to collect statistics. If you are using a GigaStor, you should allocate the vast majority of the reserved RAM for the active probe instance to packet capture.
- If you want to collect statistics or trending data, or use analysis, then allocate 90% (or even 100%) of the reserved RAM to the statistics queue buffer.
- If you want to do both, determine which you want to do more of and allocate the memory accordingly.

Recommendations for the VIAVI capture cards

There are capture card requirements and considerations if you are using a GigaStor appliance, as the appliance may have a Gen3 capture card or Gen2 capture card installed.

Here are some special configuration issues to consider when dealing with these capture cards:

- For either the Gen3 capture card or Gen2 capture card, you need a minimum of 100 MB allocated to the capture buffer of any probe instance that is bound to the capture card. Allocating less than 100 MB to a probe instance monitoring a VIAVI capture card may cause instability.
- If you are using any hardware accelerated probe instance, you must have at least 80 MB for both packet capture and the statistics queue buffer. No packets are captured if either or both are below 80 MB. 80 MB is the
minimum, but consider substantially raising this amount. The more RAM that you can allocate to packet capture and statistics, the better your GigaStor probe will perform.

♦ When using multiple probe instances on a GigaStor, ensure that only one probe instance is associated with the capture card. (If you are using virtual adapters to monitor disparate networks, then you may have more than one active instance bound to the capture card.) For performance reasons, all other probe instances should be associated with a different network card.

If you feel a capture card is not performing as expected, ensure that there is only one probe instance bound to it. If there is more than one, verify that the other probe instances are not collecting any statistics. It is possible that the probe instance you are looking at is not collecting any statistics, but one of the other probe instances may be. (This is only an issue if there are multiple probe instances connected to the Gen3 capture card or Gen2 capture card. This does not apply if the other probe instances are connected to a regular network card.)
Chapter 4: Gen3 Capture Card

The Gen3 capture card is a GigaStor appliance exclusive. Learn about its features, configuration options, supported SFP/SFP+ media types, and more.

**Hardware configuration**

Using SFP modules, the Gen3 capture card can be configured to monitor nearly any source of network traffic at a variety of connection speeds. The Gen3 capture card hardware also unlocks certain features in Observer/GigaStor.

**Understanding the capture card**

The Gen3 capture card is designed and manufactured exclusively by VIAVI. This capture card is optimized for the Observer Platform and comes pre-installed in many GigaStor hardware and probe appliances.

The Gen3 capture card is a special network adapter for high-speed packet capture. The card is full-duplex and can monitor up to eight ports\(^1\) in real time. Also, the Gen3 capture card is for capturing only, so it does not send IP traffic from any of its ports.

More features of the Gen3 capture card include:

- Hardware acceleration in Observer/GigaStor
- Deduplication to remove duplicate packets in real time
- Virtual adapters allow the creation of several logical network adapters
- Accurate and reliable time stamps
- Ports have individually configurable auto-negotiation

---

1. The number of ports varies from 2, 4, or 8, depending on the physical configuration of your hardware appliance.
♦ Able to mix-and-match 1Gb and 10Gb modules
♦ Compatible with most SFP/SFP+ module choices

**Note:** All packets captured by the probe are time-stamped immediately as they are seen by the capture card interface. The packets are then passed to the capture buffer. This ensures the most accurate time stamp.

### Supported QSFP+/SFP/SFP+ media types

The Gen3 capture card requires SFP modules. These are the supported media types.

♦ 100 Gb QSFP28 Transceivers
  - 1000BASE-SR4
  - 1000BASE-LR4
  - 1000BASE-SR

♦ 40 Gb QSFP+ Transceivers
  - 40GBASE-SR4
  - 40GBASE-LR4
  - 40Gb BIDI-SR
  - 40GBASE-RX (Receive only. For use with an optical network tap)

♦ 10 Gb Ethernet SFP+ Transceivers
  - 10GBASE-SR
  - 10GBASE-LR
  - 10GBASE-ER
  - 10GBASE-ZR
  - 10GBASE-T
  - 10 Gb Direct Attach Copper

♦ 1 Gb Ethernet SFP Transceivers
  - 1000BASE-SX
  - 1000BASE-LX
  - 1000BASE-ZX
  - 1000BASE-T (includes copper at 10/100/1000)

**Note:** For 40 Gb connections, then QSFP+ may be used and only if your exact capture card model supports it.

### How to configure the card for an optical TAP, SPAN, or other

You must make configuration changes to the capture card depending upon whether you connect to a SPAN/mirror port, a passive optical TAP, or to a switch aggregator or conversion TAP using fiber.

**Prerequisite(s):**

For fiber optic connections that require a splitter: these steps assume you are using the VIAVI optical Y-splitter cable, as it is unable to inject light back into the upstream network link and the provided steps assume the cable is being used. If
A third-party optical splitter cable is used instead when **Tx Enable** is enabled on those capture card ports, it could cause interference with the upstream network link because the cable could inject light back into the upstream network link. To summarize, the steps listed for fiber optic connections in this document might not represent the best course of action if you are using a third-party optical splitter.

Auto-negotiation sets the correct port speed between a capture card port and a network device. The network devices connected to the capture card typically include network TAPs, SPANs or mirror ports from a switch, and feeds from a network packet broker or switch aggregator. Here are some general best practices:

- Auto-negotiation must be **disabled** when connecting the capture card to a passive, fiber-optic TAP.
- Auto-negotiation must be **enabled** when connecting the capture card to copper SPAN or mirror ports.

To configure the capture card to properly connect to a network device:

1. In your version of Windows, open **Device Manager**.
2. In the tree on the right, expand **Viavi Solutions Inc. Capture Adapters**.
3. Right-click the capture card entry and choose **Properties**.
4. Click the **Advanced Properties** tab.
5. Do one of the following, and ensure the same settings are set for each capture card port that makes up a link:
   - If you are connecting a passive, optical TAP to the capture card:
     - Clear **Auto-Neg Enable** (off).
     - Clear **Tx Enable** (off).
   - If you are connecting a copper SPAN/mirror port to the capture card:
     - Select **Auto-Neg Enable** (on).
     - Select **Tx Enable** (on).
   - If you are connecting a fiber optic mirror port from a switch or conversion TAP to the capture card:
     - Clear **Auto-Neg Enable** (on).
     - Select **Tx Enable** (on).

For connecting a fiber optic mirror port from a switch, some switches need **Tx Enable** turned on for those capture card ports to establish a connection. If this results in problems, turn off **Tx Enable**. Similarly, the correct setting for **Auto-Neg Enable** can change depending on your hardware and environment, so enable or disable it if you encounter problems.
Each configured and cabled capture card port to your device(s) should establish a working connection.

When to use a SPAN/mirror port

The advantage of using a SPAN/mirror port is its cost, as a SPAN/mirror port is included for free with nearly every managed switch. A SPAN/mirror port is also remotely configurable, allowing you to change which ports are mirrored from the switch management console.

There are some limitations in using a SPAN/mirror port. Limitations of a SPAN/mirror port stem from the aggregation necessary to merge full-duplex network traffic into a single receive channel. For examples, when traffic levels on the network exceed the output capability of the SPAN/mirror port, the switch is forced to drop packets. Another reason that a SPAN/mirror port may not be the right choice is because Layer 1 and 2 errors are not mirrored and therefore never reach the analyzer. When performing network troubleshooting, seeing these errors can be important.

When monitoring with a SPAN/mirror port on a switch, the switch does three things:

- Copies both the send and receive data channels
Reconstructs an integrated data stream from the two channels
Routes the integrated signal to the send channel of the SPAN/mirror port

Each of these activities burdens the switch's internal processor. These demands on the switch's CPU have implications for both your monitoring equipment and general network performance. Using a SPAN/mirror port to capture network traffic for analysis presents the following risks:

- As total bandwidth usage for both channels exceeds the capacity of the outbound link to the analyzer, the excess traffic is dropped from the analyzer stream. There simply is not enough bandwidth to transmit both sides of the full-duplex traffic across a single standard interface.
- The switch's CPU must act as both a network switch and a packet-copier. The switch's CPU must also integrate the two data streams (send and receive) together correctly. Both packet copy/re-direction and channel integration is affected by switch load. This means the SPAN/mirror port may not deliver accurate captures when the switch is under heavy load. Monitoring a 10/100 network through a Gigabit SPAN/mirror port and analyzer does not alleviate these concerns. Also, there is no notification when the SPAN/mirror port is dropping packets or delivering inaccurate time stamps.

A SPAN/mirror port can deliver satisfactory results when used to monitor lightly used, non-critical networks. If network utilization exceeds the capacity of the outbound (analyzer) link, packet loss results—which invalidates many types of analysis, and makes monitoring for certain kinds of network activity impractical. For example, you might miss a virus signature because packets are being dropped. When analyzing a transaction or connection problem, the analyzer may detect problems where none exist because expected packets are being dropped by the SPAN/mirror port. Hardware and media errors will also be impossible to troubleshoot through a SPAN/mirror port, as these errors are not mirrored to the analyzer.

Software configuration

The Gen3 capture card hardware unlocks certain features in Observer/GigaStor. You can configure and use these settings inside the Observer application and Windows Device Manager.

How to view the capture card properties

Viewing the Gen3 capture card properties allows you to verify what you think is happening at the card level (such as SFP activity, link speed, auto-negotiation) is actually happening. Additionally, configuration changes to the card can be made here.

**Tip!** These settings can be viewed remotely using Windows RDP or an equivalent remote desktop application. You might find this useful for checking SFP and link states when physical access to the GigaStor is not feasible.

Some benefits of viewing the Gen3 capture card properties include:

- Verifying if an SFP...
  - is present and in which port.
- is active or idle.
- is operating at the speed you expect.

Verifying the board’s...
- hardware acceleration (HA) status.
- auto-negotiation settings per port.
- ID string that also contains the firmware version.
- PCIe lane speed\(^2\).
- power range (good /bad)
- operating temperature (good/bad)

Seeing configurable options for...
- per port auto-negotiation.

**Tip!** Be sure to disable auto-negotiation for TAP connections, and enable auto-negotiation for SPAN connections.

To view the Gen3 capture card properties:
1. In your version of Windows, open **Device Manager**.
2. In the tree on the right, expand **Viavi Solutions Inc. Capture Adapters**.
3. Right-click the capture card entry and choose **Properties**.

The Gen3 capture card device properties window is now visible.

**Figure 22: Gen3 capture card properties**

2. PCIe lane speed is reported per lane, and the Gen3 capture card uses multiple lanes together.
How to create virtual adapters

By default, Observer recognizes a Gen3 capture card as a single network adapter. However, you can make multiple clones of the capture card, called virtual adapters, and use each independently.

Prerequisite(s):

Your hardware appliance must have one of the following:

- Gen2 capture card
- Gen3 capture card

Each virtual adapter is a cloned Gen3 capture card that can have physical ports assigned to it in any quantity and combination. In this way, Observer can then see and use multiple network adapters as if they physically existed in your hardware appliance.

By default, you already have one virtual adapter: it matches the installed Gen3 capture card exactly, unless you accidentally deleted this virtual adapter or unassigned some of its ports. It can be recreated by following these same steps.

To create a virtual adapter:

1. In Observer, right-click the Gen3 capture card-equipped probe instance from the probe list, and click **Probe or Device Properties**.

   A Gen3 capture card-equipped probe instance shows (Gigabit) or similar after the name.

2. Click the **Virtual Adapters** tab.
3. Click **New Adapter**.
   The **Assign Ports to Virtual Adapter** window opens.

4. Type a name in the **Adapter Name** box.

5. Select physical ports from the **Available Ports** list, and click **Add**.
   You can select more than one physical port by holding **CTRL** as you click.

6. (Optional) If this virtual adapter should operate during certain days and times only, select **Schedule virtual adapter ports** and follow the prompts.
   (Optional) If you choose to set a schedule for your virtual adapter, the remaining steps in this procedure may not be followable as written.
7. (Optional) If the virtual adapter should skip (discard) duplicate packets, select **Skip duplicate packets**.

8. Select each added port, click **Edit Port**, and type a useful description for each port such as its connected device.

   This description appears in the GigaStor Control Panel in Observer.

   **Note:** If you want to filter on physical ports, an option in the hardware acceleration settings is described at .

9. Click **OK** to save the virtual adapter and close the **Virtual Adapters** window.

   Changes to virtual adapters are not be saved until **OK** is clicked in the **Virtual Adapters** window.

   The virtual adapter appears in the list of available network adapters when creating a probe instance. This allows you to assign the virtual adapter to a specific probe instance, among other benefits.

   You should create a new probe instance for any virtual adapter you create, and assign the virtual adapter to that probe instance (page 27). This is because, by default, new virtual adapters are not assigned to any probe instance, so no data is collected with that virtual adapter until the virtual adapter is assigned to a probe instance.

**How to remove duplicate packets in real time**

Use hardware acceleration on the Gen3 capture card to remove duplicate packets before they are captured to disk or acknowledged by Observer. This is called packet deduplication.

**Prerequisite(s):**

Hardware acceleration must be enabled on your Gen3 capture card for this feature to function. Hardware acceleration for your virtual adapter is enabled by default.

To use hardware acceleration to skip duplicate packets:

1. Right-click the Gen3 capture card-equipped probe instance and choose **Probe or Device Properties**.

2. Click the **Virtual Adapters** tab.

3. Click **Edit Adapter**.

4. In the **Assign Ports to Virtual Adapter** window, select **Skip duplicate packets** and click **OK**.

5. (Optional) Click **Skip Duplicate Packets Configuration**.

   The **Skip Duplicate Packets Using Hardware Accelerated Capture Adapter** dialog appears.
6. (Optional) Select how duplicate packets are recognized by the Gen3 capture card and click **OK**.

   **Example:** (Optional) For example, by selecting **Examine IP time to live (TTL)**, the packet time to live is considered when determining a duplicate packet. If the option is cleared, TTL is ignored for all consideration of what is, and what is not, a duplicate packet.

7. Click **OK** to enable packet deduplication.

   The Gen3 capture card now skips duplicate packets that it receives on the active instance. The duplicate packets will not be saved to disk or acknowledged by Observer.

**How to assign physical ports to probe instances**

By default, the active instance monitors network traffic from every physical port of your capture card—all the traffic is aggregated. If you want to instead “divide” your monitored network traffic by physical ports, to help you monitor certain
SFPs separately from others, then you can use virtual adapters to assign specific physical ports to probe instances.

**Prerequisite(s):**

Your hardware appliance must have one of the following:

- Gen2 capture card
- Gen3 capture card

For example, suppose you are deploying an 8-port Gen3 capture card as follows:

- Ports 1-4 are monitoring a collection of trunked links
- The remaining ports are each connected to the SPAN (or mirror) port on a switch

In this scenario, it makes sense for Observer to view ports 1-4, for example, as a single stream of network traffic and to separate each of the four remaining ports into separate data streams. Virtual adapters are a convenient way to accomplish this separation or aggregation in real time, rather than depending on filters to sort through the traffic post-capture.

These are the general steps for assigning physical ports to a probe instance:

- Create a virtual adapter (or have one already).
- Assign physical ports to this virtual adapter.
- Set a probe instance to use this virtual adapter as its NIC.

**Tip!** As a general reminder, you risk severe performance loss when using more than one active instance. These instructions do not create multiple active instances.

To assign physical ports to a specific probe instance:

1. In Observer, right-click the Gen3 capture card-equipped probe instance from the probe list, and click **Probe or Device Properties**.

   A Gen3 capture card-equipped probe instance shows (Gigabit) or similar after the name.

2. Click the **Virtual Adapters** tab.
3. Select a virtual adapter, and click **Edit Adapter**.
4. Select physical ports from the **Available Ports** list, and click **Add**.
   
   You can select more than one physical port by holding **CTRL** as you click.
5. Click **OK** to return to the **Virtual Adapters** window.
6. Click **OK** to save the virtual adapter and close the **Virtual Adapters** window.

   Changes to virtual adapters are not be saved until **OK** is clicked in the **Virtual Adapters** window.

The virtual adapter appears in the list of available network adapters when creating a probe instance. This allows you to assign the virtual adapter to a specific probe instance, among other benefits.
Next, you should change the monitored network adapter (page 27) of a probe instance to use the virtual adapter.

**How to change the monitored network adapter**

If your probe has multiple network cards in it, you can choose which card you want to monitor.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on VIAVI or third party hardware.

**Note:** If you have a network card in your system, but it is not being seen or recognized by Observer, follow the instructions in No network adapter available (page 104).

**Tip!** If you are seeing only broadcast traffic, you do not have the correct network card selected or you do not have your switch port configured correctly as a SPAN/mirror port. Change the network adapter you are monitoring or configure the SPAN/mirror port.

- When choosing the monitored adapter from within Observer for all probe versions:
  1. In the probes list, select the probe instance.
  2. Choose .
     The **Select Network Adapter** window appears.
  3. Select the network adapter you want to monitor, and click Select.

- When choosing the monitored adapter on the probe for Multi Probe and Expert Probe:
  1. Click **Adapters and Redirection**.
  2. Select your probe instance and click **Configure Adapter/Redirection**.
     The **Edit Probe Instance** window appears.
  3. In the **Selected Network Adapter** area, change the network card you are monitoring.

The probe instance is now using the newly selected adapter.

**Understanding hardware acceleration**

*Hardware acceleration* optimizes a GigaStor active instance for its fastest possible operating speed by using the Gen3 capture card instead of the system CPU.

*Hardware acceleration significantly increases the performance of an active instance than without it.* By using hardware acceleration with the Gen3 capture card, the fastest capture rates and post-capture analysis can be achieved in your GigaStor hardware or probe appliance. Turning off hardware acceleration is not recommended, as packet capture performance will be greatly degraded because this work is offloaded from Gen3 capture card to the CPU instead where it competes for resources.

**Do not turn off hardware acceleration unless you have a specific need to.** The feature provides performance benefits only; there are only advantages to
gain by using hardware acceleration. However, two situations require that you disable hardware acceleration on the active instance:

1. If you need the GigaStor active instance to filter network traffic in real time using a “deeper” set of filters than the following:
   - MAC/IP Address
   - MPLS
   - Port
   - VLAN Tag (802.1Q)
   - VNTag

   It is a best practice to use the supported broad filters (page 90) listed or no filters when capturing real-time network traffic with the GigaStor active instance. As soon as the network traffic is written to the RAID array, it becomes available for data mining and more complex filters can be used. If unwanted traffic is entering your GigaStor system, it is instead recommended that the connected switches, SPAN, or aggregator switch be configured to discard those packets before they reach the Gen3 capture card.

2. If you have an eight (8) port Gen3 capture card and intend to create one virtual adapter for each physical port, then hardware acceleration must be disabled. This is because only four virtual adapters can be created while hardware acceleration is enabled. In practice, this is not a typical setup, and better use of your hardware is gained by leaving hardware acceleration enabled than separating more than four ports of traffic.

Tip! You can verify if hardware acceleration is enabled by viewing the capture card properties (page 78).

The active instance is the only probe instance that can be configured for hardware acceleration. This means you cannot configure a passive instance to use hardware acceleration—the option simply does not exist—but passive instances can always be created from your hardware-accelerated active instance. Each GigaStor appliance with a Gen3 capture card is configured to use the card for the active instance, so the best capture performance is ready out-of-the-box.

Hardware acceleration does not affect or speed-up statistics-based features like Network Trending. Statistic-based features behave exactly the same whether hardware acceleration is enabled or disabled, and this is because hardware acceleration affects packet capture modes only.

Note: When allocating memory for any probe instance with the VIAVI capture card as the chosen adapter, at least 80 MB of memory must be allocated to both the capture buffer and statistics queue buffers. Failure to do so will result in the inability to capture data. This must also be followed for any Gen3 capture card that has hardware acceleration enabled.

How to enable hardware acceleration

Hardware acceleration must be turned on for certain features in Observer and the GigaStor Control Panel to become usable. Hardware acceleration is exclusive to the Gen3 capture card.
Prerequisite(s):
To complete these steps, your probe instance list must show the active instance of your GigaStor probe. This can be accomplished by using Windows Remote Desktop to log on to the GigaStor system—so you can see the active instance directly—or by temporarily redirecting the active instance of the GigaStor system to your Observer analyzer.

Hardware acceleration is enabled by default on the local active instance of your GigaStor system. If you find that hardware acceleration is disabled, you can re-enable hardware acceleration.

To enable hardware acceleration mode:

1. In the probe instance list, in Observer, right-click the active probe instance and click **Probe or Device Properties**.
2. Click the **Virtual Adapters** tab.
   
   **Tip!** Using the Expert Probe interface instead? Find this window tab at **Options > Virtual Adapters**.
3. Select **Enable Hardware Acceleration**.

   Figure 26: Hardware acceleration is enabled

   ![Hardware acceleration enabled](image)

   The active instance now uses hardware acceleration provided by the Gen3 capture card.

   To further verify that hardware acceleration is enabled, you can view the capture card driver properties (page 78) in Windows Device Manager.

Redirecting a probe instance

Your local Observer may already have local probe instances defined, but you can add numerous remote probes, including GigaStor, too. You must first redirect the remote probe to your local Observer.
A probe may have multiple probe instances, which are useful if you need multiple users using the same probe simultaneously or if you have specific needs for each probe instance (for instance, packet capture, trending, and so on). When you connect to a probe, ensure you select the probe instance you need and not one being used by someone else.

**Note:** Probe redirection can either be password protected or disabled, depending on the target probe.

To redirect a probe instance, complete the following steps:

2. Do one of the following:
   - If you see a remote probe instance you want to redirect, skip directly to step 6.
   - If your list is empty or missing the remote probe instance you want to redirect, proceed to step 3.

3. Click **New**.
   
The *Edit Remote Probe Entry* dialog appears.

4. Type the IP address, or DNS address, of the remote probe.
   
   If you type a DNS name, it resolves to its IP address.

5. If necessary for probe access, type a user name and password, and click **OK**.

Figure 27: Credentials may be needed
6. Select the remote probe instance from the list, and click **Redirect Selected Probe Instance(s)**.

Allow time for the remote probe to redirect. How long this operation can take is limited by a timeout countdown.

The probe instances of the remote probe are shown.

7. Select a probe instance from the list, and click **Redirect Selected Instance**.

8. Select the **Redirect to this Observer**, and click the **Redirect** button.

9. Close the **Probe Instance Redirection** window.

If the operation succeeds, the remote probe instance is now redirected to the local Observer. Now you can use the remote probe instance just as you would if it was running on your local machine.

---

**Hardware-accelerated mode restrictions**

The Gen3 capture card has a very short list of restrictions while running in hardware-accelerated mode. These restrictions are designed to keep your hardware operating at peak performance when hardware acceleration is enabled.

While a Gen3 capture card runs in hardware-accelerated mode, it cannot:

- Connect itself to multiple probe instances without the aid of virtual adapters (page 80).
- Use overly complex filters that would affect hardware-accelerated performance (rare occurrence). An error message will alert you if the filter is too complex for hardware acceleration, but the filter can be rewritten or tweaked to be accepted.
Use software-based pre-filters. They are mutually exclusive; only one may be used.

Affect statistics-based information, such as Network Trending.

There are two types of filtering that occurs in GigaStor: hardware filtering on the capture card and software filtering in Observer. Hardware filtering only affects which packets are captured on the capture card and saved to the RAID; it does not work with any statistics-based filtering that may occur in the Observer software, such as for Network Trending, Bandwidth Utilization with Filter, and so on. Any packets excluded by the hardware filter are never saved to disk and searchable by the software. In general, you want your hardware filter to allow as many packets through as possible. This ensures the largest number of packets are available for troubleshooting. In some cases, it is desirable to use hardware filtering because you know you do not need certain types of traffic captured and saved by GigaStor. Hardware filtering is only available when using hardware acceleration; it also disables the use of software-based pre-filters. Software filtering has two of its own possibilities when using hardware filtering: 1) sifting through packets after they were written to the RAID by the capture card and 2) controlling what is available for network trending when collecting statistics.

<table>
<thead>
<tr>
<th>Hardware filtering</th>
<th>Filters packets before they are saved to the RAID. This disables the ability to use software pre-filters in Observer, which rely on the CPUs rather than the capture card to do the processing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software post-filtering of packets</td>
<td>Filters packets saved to disk by the capture card, which may or may not have a hardware filter applied. See Observer Filters.</td>
</tr>
<tr>
<td>Software filtering of network trending</td>
<td>Filters statistics-based trending data, which is entirely unrelated to packet capture. See Choosing your network trending types.</td>
</tr>
</tbody>
</table>

These are the filtering types usable on a hardware-accelerated virtual adapter:

- MAC/IP Address
- MPLS
- Port
- VLAN Tag (802.1Q)
- VNTag

**Features that require hardware acceleration**

Some functions or features of your hardware appliance require that hardware acceleration is turned on.

These cannot operate if hardware acceleration is turned off:

- Real-time packet deduplication
- Physical ports reused in multiple virtual adapters
- Hardware filters
- Disk read and write speeds that match advertised values
Capture card device properties

The capture card device properties in Windows Device Manager shows a mix of standard driver information (like any connected device) and custom information about your capture card.

General

The **General** tab lists basic information about the capture card.

**Figure 29: General**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device type</td>
<td><strong>Device type should state</strong> Viavi Solutions Inc. Capture Adapters.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td><strong>Manufacturer should state</strong> Viavi Solutions.</td>
</tr>
<tr>
<td>Location</td>
<td><strong>Location indicates the PCI bus number that the capture card is using.</strong></td>
</tr>
<tr>
<td>Device status</td>
<td><strong>If Windows itself has a problem with the capture card, messages appear here indicating the problem. Device status states</strong> <em>This device is working properly when no Windows problems exist.</em></td>
</tr>
</tbody>
</table>

Current State

The **Current State** tab displays capture card health, SFP presence, and established port speeds.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP state</td>
<td>SFP state shows capture card ports that have a supported SFP installed (page 75), if that SFP is operational, and if the SFP is fiber (F) or copper (C). If a capture card port does not have an SFP installed, its icon remains dimmed.</td>
</tr>
<tr>
<td>Link state</td>
<td>Link state is a way to see if the Gen3 capture card is synchronized with the SPAN/TAP/Observer Matrix. If the link state is not green, there is a problem. Click the <strong>Advanced Settings</strong> tab to try and change the adapter speed or auto-negotiation.</td>
</tr>
<tr>
<td>SFP power (dBm)</td>
<td>Actual amount light power seen by the transceiver in the capture card, measured in decibels-milliwatts. With this information you can determine if the signal strength is strong enough to transmit the traffic or if it is too low and is the cause of dropped packets.</td>
</tr>
<tr>
<td>Enabled (Autonegotiation)</td>
<td>The icon is lit when auto-negotiation is enabled for that capture card port. Conversely, the icon is dimmed when auto-negotiation is disabled for that capture card port.</td>
</tr>
<tr>
<td>10 Gig</td>
<td>This icon is lit when a 10 gigabit connection is established.</td>
</tr>
<tr>
<td>1 Gig</td>
<td>This icon is lit when a 1 gigabit connection is established.</td>
</tr>
<tr>
<td>100 Mb</td>
<td>This icon is lit when a 100 megabit connection is established.</td>
</tr>
<tr>
<td>10 Mb</td>
<td>This icon is lit when a 10 megabit connection is established.</td>
</tr>
<tr>
<td>PCIe lane speed</td>
<td>The reported 1x lane bus speed of the PCIe slot used by the capture card. Multiple lanes are used by the capture card, so this value represents a fraction of actually available bandwidth between the capture card and the motherboard.</td>
</tr>
<tr>
<td>Temperature</td>
<td>A green icon means the temperature of vital board components is lower than 75°C and therefore normal. Seeing a yellow icon is a caution that this temperature has risen above 75°C. A red icon is shown when this temperature is greater than 80°C, and you</td>
</tr>
</tbody>
</table>
### Field Description

- **Power**: This icon shows a red color if there is a power problem. A power problem could occur if the 12v power supply (PSU) rail, typically for MOLEX and auxiliary connections, is operating out-of-range and could indicate a dying power supply. A power problem could also be caused by the PCIe slot providing too little or too much wattage to the capture card relative to the PCIe specification. This could indicate a motherboard problem or a dying PSU. A green icon means that power to the card is normal.

- **Board ID**: The unique ID of the capture card is shown here.

- **System ID**: The system ID is shown here.

---

**Figure 31: Explanation of lights**

<table>
<thead>
<tr>
<th>Explanation of Lights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>When SFP is Present</strong></td>
</tr>
<tr>
<td>Input is active</td>
</tr>
<tr>
<td>Input is inactive</td>
</tr>
<tr>
<td><strong>When SFP is not Present</strong></td>
</tr>
<tr>
<td>Disabled</td>
</tr>
<tr>
<td><strong>SFP Lights</strong></td>
</tr>
<tr>
<td>Copper installed</td>
</tr>
<tr>
<td>Fiber installed</td>
</tr>
<tr>
<td><strong>Link Lights</strong></td>
</tr>
<tr>
<td>10 Gg</td>
</tr>
<tr>
<td>1 Gg</td>
</tr>
<tr>
<td>100 Mb</td>
</tr>
<tr>
<td>10 Mb</td>
</tr>
<tr>
<td>No link</td>
</tr>
</tbody>
</table>

---

**Advanced Settings**

The **Advanced Settings** tab allows you to view and modify auto-negotiation and port Tx settings for the capture card. Each port has its own settings.
Figure 32: Advanced Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable (Port)</td>
<td>Each box represents a physical port on the capture card. These cannot be modified.</td>
</tr>
<tr>
<td>Auto-Neg</td>
<td>Each box represents the auto-negotiation setting for a port on the capture card. If selected, auto-negotiation for this port is turned on. If cleared, auto-negotiation is disabled for this port. See How to configure the card for an optical TAP, SPAN, or other (page 75) when using this setting.</td>
</tr>
<tr>
<td>Enable Port Tx</td>
<td>Each box represents a port on your capture card. All are enabled, and none can be disabled. See How to configure the card for an optical TAP, SPAN, or other (page 75) when using this setting.</td>
</tr>
</tbody>
</table>

**Driver**

The **Driver** tab
**Figure 33: Driver**

The **Details** tab lists device properties that are reported by the driver.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver provider</td>
<td>Driver provider should state <em>Viavi Solutions</em>.</td>
</tr>
<tr>
<td>Driver date</td>
<td>Shows the date that your currently installed capture card drivers were made.</td>
</tr>
<tr>
<td>Driver version</td>
<td>Shows the version of your currently installed capture card drivers. These do not always match your application versions for the Observer Platform.</td>
</tr>
<tr>
<td>Driver signer</td>
<td></td>
</tr>
</tbody>
</table>
### Figure 34: Details

The **Events** tab shows driver events like when a capture card driver is installed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Lists each device property that can be viewed.</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the value of the selected property as reported by the device driver.</td>
</tr>
</tbody>
</table>
Figure 35: Events

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>Each Windows event regarding the capture card is logged. This can help you understand when the drivers were updated and can be useful when troubleshooting.</td>
</tr>
<tr>
<td>Information</td>
<td>The full event message shows here for the selected Windows event.</td>
</tr>
</tbody>
</table>

Resources

The **Resources** tab lists the interrupt request number and memory range assigned to the capture card. These values cannot be modified.
How to identify your GigaStor

The capture card found in a GigaStor appliance tells you a great deal about the vintage and the capabilities of the appliance.

There are two versions of GigaStor under active maintenance. A purple version called GigaStor Gen3 and a blue version called GigaStor Gen2. The “Gen3” or “Gen2” refers to the capture card used in the appliance.

If you can see the appliance, you can easily discern which version you have by looking at its color; however, if you do not have physical access to it then you must view the capture card properties (page 92). Even if you can see the color you may not be able to identify which model of the capture card you have.

The Windows operating system used on the GigaStor appliance is a useful clue about the version, but it is not conclusive and cannot be used alone.

1. In your version of Windows, open Device Manager.
2. Find and expand one of these.
   - Viavi Solutions Inc Capture Adapters
• Network Instruments Capture Adapters

3. Use the information in Capture card details (page 100).

With this information you can precisely know what components are in the system. Use that knowledge to learn what their capabilities are.

Capture card details

Using names, drivers, and manufacturer information helps identify the capture card found in your system.

Table 14. Capture card versions in GigaStor Gen3

<table>
<thead>
<tr>
<th>Name</th>
<th>Internal Name</th>
<th>Driver Name</th>
<th>Manufacturer Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIAVI Solutions 1/10 Gigabit Ethernet Capture Adapter Gen3</td>
<td>oneTenGig2015</td>
<td>tenGig2015.sys</td>
<td>VIAVI Solutions, Inc.</td>
</tr>
</tbody>
</table>

Table 15. Capture Cards versions in GigaStor Gen2

<table>
<thead>
<tr>
<th>Name</th>
<th>Internal Name</th>
<th>Driver Name</th>
<th>Manufacturer Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Instruments 40 Gigabit Ethernet Capture Adapter Gen2</td>
<td>fortyGig2010</td>
<td>fortyGig2010.sys</td>
<td>Network Instruments, LLC.</td>
</tr>
<tr>
<td>Network Instruments 10 Gigabit Ethernet Capture Adapter Gen2</td>
<td>tenGig2010</td>
<td>tenGig2010.sys</td>
<td>Network Instruments, LLC.</td>
</tr>
<tr>
<td>Network Instruments 1 Gigabit Ethernet Capture Adapter Gen2</td>
<td>oneGig2010</td>
<td>oneGig2010.sys</td>
<td>Network Instruments, LLC.</td>
</tr>
<tr>
<td>Network Instruments 10 Gigabit Ethernet Capture Adapter Gen2</td>
<td>tenGig2007</td>
<td>tenGig2007.sys</td>
<td>Network Instruments, LLC.</td>
</tr>
<tr>
<td>Network Instruments 1 Gigabit Ethernet Capture Adapter Gen2</td>
<td>oneGig2007</td>
<td>oneGig2007.sys</td>
<td>Network Instruments, LLC.</td>
</tr>
<tr>
<td>Network Instruments 1 Gigabit Ethernet Capture Adapter Gen2</td>
<td>oneGig2005</td>
<td>oneGig2005.sys</td>
<td>Network Instruments, LLC.</td>
</tr>
</tbody>
</table>

1. Some capture cards have the same name and can only be distinguished by their internal name or driver.
Can I upgrade a Network Instruments-manufactured, blue GigaStor to Observer 17.2 or later?
Yes, if you have an active maintenance contract. No new features are available on the Gen2 capture card as a result of this name change.

Can I put a Gen3 capture card in a Network Instruments-manufactured, blue GigaStor?
No, the Gen3 capture card is only available in the GigaStor Gen3 appliance.

Are firmware upgrades separately available?
Firmware and driver updates are only provided through the Observer installation program. Not every release contains firmware or driver updates; in fact, most do not.
Chapter 5: Troubleshooting

Troubleshooting common issues

Use the information in this section to assist you if you have a problem with your probe not connecting to your analyzer, your probe does not have a network adapter available, or if you are using an nTAP and want to capture NetFlow traffic or several other common issues.

If you feel your probe is slow, see Troubleshooting a slow probe system (page 103).

Although most installations of Observer Analyzer proceed without any trouble, due to the vast number of network configurations and hardware/software options that Observer supports, sometimes difficulty arises.

If you experience trouble in setting up Observer, keep a number of things in mind.

First and foremost, try to simplify your configuration in any way possible. This means if you have a screen saver loaded, disable it. If you are running some network add-on peer-to-peer jet engine turbo stimulator, remove it. This does not mean that you will not be able to use Observer with your other products but, if you can determine where the problem is, you can focus on that piece of the puzzle and you may be well on your way to solving the problem.

Second, do not trust anyone or anything. The only way to really know what your hardware settings are is to have the card or device in one hand and the documentation in the other. Programs which discover interrupts and other settings only function properly when everything is working correctly — exactly when you do not need them. Do not blindly trust other network drivers — they may or may not be reporting the correct information.

Third, do not, under any circumstances, share interrupts, I/O ports, or memory addresses between adapters. No matter what has worked before or what
might work in the future, sharing interrupts or memory settings is not a valid configuration.

Troubleshooting checklist:

Does your network work without any Observer programs or drivers loaded? If not, check your network installation instructions. After your network appears to be running correctly, install Observer again. Try installing Observer on a different system and see if you experience the same problem. This does not mean that you will not be able to use Observer on the desired system. It may give you some insight into the problem that you are having.

Troubleshooting a slow probe system

If a probe is overloaded, consider whether any of the following affect the system. You can clear these one at a time to see if that resolves the system’s issue.

Although all of the settings discussed in this section are configured in Observer, they are saved to the probe.

♦ A scheduled capture can be causing a system slow down. Determine if any scheduled capture is occurring. On the Home tab, in the Capture group, click Live > Packet Capture and then Settings > Schedule.

♦ Some extra processing happens when you have triggers and alarms configured. Determine what alarms are enabled by clicking the Alarm Settings button in the lower left.

♦ Are you running real-time Expert Analysis? Observer requires some processing resources to get through the data, which could be a lot of data. Real-time expert processes data as it is received. This requires continuous processing of incoming data while the real-time expert is running.

♦ Are you collecting combined station statistics or protocol distribution summary for your network? If so, these could be causing the system to slow down. To determine if you are, click the File tab, and click Options > General Options. Scroll to Startup and runtime settings and clear these settings, if necessary:
  • Collect combined station statistics at all times
  • Collect protocol distribution for the whole network

♦ Are you collecting network trending statistics? If so, is the sampling divider less than 10? If so, increase the sampling divider to 10 or greater. To determine your sampling divider, on the Home tab, in the Capture group, click Network Trending > Network Trending. Then click Settings > General tab. In the Collection Settings section, change the sampling divider.

A probe is not connecting to the analyzer or vice versa

If the probe is not connecting, it could be one of several reasons. The log window in Observer has useful information to give you an idea of why the connection is failing.

Verify the following:

♦ The probe is licensed. See Licensing and updating (page 21).
♦ Check that the Observer Platform ports are open on the firewall and if traffic is actually passing through it. Observer uses these ports to communicate with the probe. See or depending on your version. Check any local system firewall as well as any network firewall. See also the information in Suspected NAT or VPN issues (page 107).

♦ Check that the security certificates are trusted between the Observer and the probe. If the settings do not match, you might get a message that says "Probe redirection Error <IPAddress> Authentication Negotiation Error" or "Probe authentication failed <IPAddress>". Either a certificate is untrusted by one of the assets or a certificate is pending your approval. In Observer, click and click the Security tab. Verify that the specific certificates are in a trusted state.

♦ The probe and Observer are within the same minor build range.

♦ You can access the VLAN if the probe or Observer are on different VLANs. There is nothing you need to configure in Observer or the probe to enable a connection when they are on different VLANs. However, if you do not have network permissions to access a probe on a different VLAN, it is a network configuration issue (usually for security reasons) and you should contact the network administrator.

No network adapter available

After starting Observer, if you do not see any available adapters listed in the "Select Network Adapter" list, it means your NIC does not have the necessary driver or VMONI Protocol settings installed. Use this information to enable your adapter and to install the proper drivers.

1. If Observer is running, close it.
2. Ensure you are logged in to the system with an account with administrator rights.
3. From the Windows Start menu, choose Control Panel > Network and Sharing Center.
4. Click Change Adapter Settings.
5. Right-click any of the Local Area Connections and choose Properties.
6. Look at the list of installed components to verify that the VMONI Protocol Analyzer is listed. Then do one of the following:
   • If it is not installed, skip to step 7.
   • If the VMONI driver is listed, remove it. Select VMONI Protocol Analyzer and click the Uninstall button. After the VMONI driver is removed, restart the system and continue with step 7.
7. From the Local Area Connection Properties (step 5), choose Install > Protocol > Add > VIAVI – VMONI Protocol Analyzer and click OK. If the VMONI driver is not listed, click Have Disk, then browse to the VMONI.SYS file located in the Observer directory on your hard drive, select it, and click OK.
   The VMONI Protocol Analyzer will now be available to install.
8. Restart the computer after you have completed installing the driver.

You should now be able to select an adapter when starting Observer.
## Integrated adapters report all sent packets with bad TCP checksum

**Symptoms:** All TCP packets sent from Observer or probe station across an integrated network adapter contain bad TCP checksums.

**Causes:** Default driver settings for the card are incorrect. You must update the driver and then disable the “Offload Transmit TCP Checksum” option.

**Solutions:** Upgrade the driver for the integrated network adapter to the Network Instruments/Intel Pro 1000 adapter driver. This driver is located in the: `<Observer installation directory>\Drivers\IntelPro1000` directory.

1. After upgrading the driver, right-click the adapter and go to **Control Panel > Network Connections > Properties**.
2. On the General tab, click the **Configure** button.
3. Click the **Advanced tab** and find the Offload Transmit TCP Checksum option and disable it.
4. Restart your system.

## “No VLAN” shown while using a Gigabit NIC

**Symptoms:** “No VLAN” is displayed in VLAN Statistics and/or no 802.1Q tag information is shown in your decode. The network adapter you use to capture traffic is a Gigabit NIC.

**Causes:** Observer is not seeing the 802.1Q tag on packets being captured. This is sometimes caused by your switch not sending tagged packets to Observer. See [VLAN Statistics tool is not working](#) for explanation/resolution before proceeding.

**Solutions:** If you are using a Gigabit NIC to capture the traffic and you have checked the switch configuration, then try using this solution. For BCM5751M NetXtreme Gigabit chips found in IBM T43, HP laptops, and Dell Latitude laptops; there is a registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet` that can cause the driver and chip not to strip the 802.1Q headers. To set that key, you must find the correct instance of the driver in Windows registry and change it.

1. Open the Windows registry editor. **Start > Run > Command** and type `regedit`.
2. Search for “TxCoalescingTicks” and ensure this is the only instance that you have.
3. Right-click the instance number (e.g., 0008) and add a new string value.
4. Type `PreserveVlanInfoInRxPacket` and give it the value `1`.
5. Restart the computer.

The Gigabit NIC no longer strips VLAN tags, so the symptom in Observer is resolved.

## VLAN Statistics tool is not working

**Symptoms:** “No VLAN” is the only VLAN ID that shows up in the VLANs column in VLAN Statistics. You are not seeing all VLANs you have on the network.
**Causes:** To display VLAN Statistics, Observer checks each packet for a VLAN tag; if no tag is present, the packet is logged as “No VLAN.” Both 802.1Q or ISL VLAN tags are stripped unless the SPAN destination port to which the analyzer is attached has been configured to include VLAN tags.

**Solutions:** Configure the switch to retain the VLAN tags through the monitor port. This may be an option in the Mirror or SPAN command on the switch, or you may have to configure the port as a trunk prior to defining it as a SPAN port. Even if the switch is monitoring a trunk or uplink port it may strip VLAN tags unless you configure that port to retain the tags. Refer to the documentation from your switch for details on configuring VLANs, trunks, and analyzer ports.

If connecting Observer to a Cisco switch, see the following link (it does require a TAC account): http://www.cisco.com/en/US/customer/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml.

If you use a Cisco Catalyst 4500/4000, 5500/5000, or 6500/6000 Series Switch running CatOS you must configure the destination port as a trunk port prior to configuring the SPAN port using the set trunk and set span commands:

```
set trunk
module/port
[on | off | desirable | auto | nonegotiate]
[vlan_range] [isl | dot1q | negotiate]

set span
source_port
destination_port [rx | tx | both]
```

For example, to configure module 6, port 2 for monitoring an 802.1Q VLAN setup, you would enter the following commands:
```
switch (enable) set trunk 6/2 nonegotiate dot1Q
switch (enable) set span 6/1 6/2
```

For Cisco Catalyst 2900/3500, 4500/4000 and 5500/5000 Series Switches Running IOS 12.1 or later, encapsulation forwarding is set as a part of the SPAN command, which has the following syntax:
```
monitor session session_number (source | destination)
interface type/num  [encapsulation (dot1q | isl)]
```

To monitor 802.1Q VLAN traffic passing through Fast Ethernet 02 via a SPAN port set up on Fast Ethernet 0/6, you would enter the following commands:
```
C4000 (config) # monitor session 1 source interface fastethernet 0/2
C4000 (config) # monitor session 1 destination interface
fastethernet 0/6  encapsulation dot1Q
```

For a 6500/6000 Series Switch running Native IOS 12.1 or later you must configure the destination port as a trunk port prior to configuring the SPAN, which have the following syntax:
```
C6500(config)#Interface Type slot/port
C6500(config-if)#Switchport
C6500(config-if)#Switchport trunk encapsulation { ISL | dot1q }
C6500(config-if)#Switchport mode trunk
C6500(config-if)#Switchport nonnegotiate
```
To monitor 802.1Q VLAN traffic passing through Fast Ethernet 02 via a SPAN port set up on Fast Ethernet 0/6, you would enter the following commands:

```
C6500 (config) # interface fastethernet 0/6
C6500 (config-if) # switchport
C6500 (config-if) # switchport trunk encapsulation dot1q
C6500 (config-if) # switchport mode trunk
C6500 (config-if) # switchport nonnegotiate
C6500 (config-if) # exit
C6500 (config) # monitor session 1 source interface fastethernet 0/2
C6500 (config) # monitor session 1 destination interface fastethernet 0/6
```
If the probe is outside the network where Observer is running, you must forward port 25901 from the probe’s address to the system running Observer.

When redirecting the probe, you must specify the NAT outside IP address instead of the address that Observer puts in automatically. By default, Observer tries to use its local IP address, which the probe will not be able to find. Select “Redirect to a specified IP address” in the Redirecting Probe or Probe Instance dialog and type the VPN client’s IP address.

**Running Observer passively affects NetFlow**

When analyzing a link using a TAP, which is common, Observer runs “passively.” Passive operation guarantees that analysis will not affect the link; however, it does have some implications when running NetFlow. Because there is no link over which the system can transmit packets or frames, the following features are unavailable:

- Traffic Generation
- Collision Test
- Replay Packet Capture

**Daylight Savings Time**

Observer is not coded with a specific date in mind. Daylight Savings Time is controlled by the operating system. When the clock rolls backwards or forwards Observer rolls with it, with one exception: packet capture/decode.

Packet capture provides nanosecond time resolution, which none of the rest of the product does. Because of this, packet capture does not rely on the system clock to provide time stamps. It relies on the processor time ticks. When Observer opens it requests the system time and the number of processor time ticks and uses those. This allows Observer to know what date and time it is when a packet is seen.

Because the Observer only asks the operating system for the system time when Observer is started, packet capture does not know that the time has jumped forward or backward. To get this to happen you need restart Observer after the time change. It is that simple.

**Configuring Cisco 6xxx switches using a SPAN port to a full-duplex Gigabit Probe**

When using a full-duplex Gigabit Probe to capture directly from a SPAN/mirror port, use a straight-through cable from the Gigabit port on the switch to either port A or B on the Gigabit card in the probe. Do not use the Y-cable or TAP (the TAP and Y-cable should only be used inline).

To use Observer with the Cisco 6xxx switch, you must disable auto negotiation. With auto negotiation enabled, the switch and probe may create a link when first starting the probe, but if the cable is unplugged or if a configuration change to the SPAN/mirror port is applied, you will lose connectivity to the switch. To turn auto negotiation off on the switch, follow the directions based on the OS you are using on your switch.
Tip! Disabling Auto Negotiation is recommended on all models/brands of switches when using a SPAN/mirror port to a full-duplex Gigabit Probe.

**Cisco CatOS switches**

1. To disable port negotiation:
   
   ```
   Console> enable
   Console>(enable) set port negotiation mod_num/port_num disable
   ```

2. To verify port negotiation:
   
   ```
   Console.(enable) show port negotiation [mod_num/port_num]
   ```

3. To enable port negotiation (should you remove the gigabit Observer product from the switch):
   
   ```
   Console>(enable) set port negotiation mod_num/port_num enable
   ```

**Cisco IOS switches**

1. To disable port negotiation:
   
   ```
   Console> enable
   Console# configure terminal
   Console(config)# interface gigabitethernet mod_mun/port_num
   Console(config-if)# speed nonegotiate
   ```

2. To verify port negotiation:
   
   ```
   Console# show interfaces gigabitethernet mod_mun/port_num
   ```

3. To enable port negotiation (should you remove the gigabit Observer product from the switch):
   
   ```
   Console(config)# interface gigabitethernet mod_mun/port_num
   Console(config-if)# no speed nonegotiate
   ```
Many of the tools in Observer have the ability to import and export settings. You can use this functionality to back up or restore certain parts of your software configuration.

**Backing up your GigaStor settings**

You can back up most Observer settings and configuration data. Backups are useful when migrating to new hardware, upgrading the operating system, or recovering from data loss.

**Caution:** If you are using data encryption on your GigaStor system, you must save the encryption keys before upgrading the operating system. Because the keys are typically stored on the operating system drive, they will be lost during the upgrade process. If you do not have a copy of the keys elsewhere, you will not be able to access stored data (packets) after the upgrade is complete.

Your Observer may not have each directory referenced in this topic, but you can back up those that are present. Use whatever backup method is best for you.

To back up many Observer settings and files, do the following:

- Copy the files and directories in Table 16 (page 110) to a backup location. This must be a location other than the operating system drive of the system you are planning to upgrade.

<table>
<thead>
<tr>
<th>Directory or file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Trending</td>
<td>C:\Program Files\Observer\NetworkTrending</td>
</tr>
<tr>
<td></td>
<td>This contains your Network Trending data. If you have changed the default location for Network Trending data, you must to...</td>
</tr>
<tr>
<td>Directory or file</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Protocol Definitions</strong></td>
<td>C:\Program Files\Observer\ProtocolDefs. This contains any modifications or additions you have made to the protocol definitions list for each probe instance. Back up in all cases.</td>
</tr>
<tr>
<td><strong>Multicast Definitions</strong></td>
<td>C:\Program Files\Observer\MulticastDefinitions. This contains the templates for defining trading multicast streams for Network Trending. Back up if you use trading multicasts in Network Trending.</td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>C:\Program Files\Observer\Settings. This contains alarms and triggers. Back up if you heavily use alarms or have alarm/trigger customizations that need to be retained.</td>
</tr>
<tr>
<td><strong>SNORT Rules</strong></td>
<td>C:\Program Files\Observer\Forensics. This contains your SNORT information, such as rules, for detecting malicious activity in your packet captures. Back up if you use SNORT.</td>
</tr>
<tr>
<td><strong>Expert Thresholds</strong></td>
<td>C:\Program Files\Observer\ExpertSettings. This contains your thresholds stored in Expert settings. These include TCP/UDP events and some triggers for problem identification. Back up if you have modified any Expert thresholds and want to retain those customizations.</td>
</tr>
<tr>
<td><strong>SNMP</strong></td>
<td>C:\Program Files\Observer\SNMP. This contains any custom MIBs, compiled MIBs, request files and SNMP trending data. Back up if you have made SNMP changes or have SNMP trending data. Use the Folders tab in to verify which folder is used for SNMP.</td>
</tr>
<tr>
<td><strong>Address Tables</strong></td>
<td>C:\Program Files\Observer\LocalAddressTable. This contains your Discover Network Names list. Back up if you have run Discover Network Names and have saved the alias list. C:\Program Files\Observer\ProbeAddressTable. This contains the Discover Network Names list from any remote probe that has connected to this Observer analyzer. Back up if you have run remote Discover Network Names and saved the alias list.</td>
</tr>
<tr>
<td><strong>Scripts</strong></td>
<td>C:\Program Files\Observer\Scripts. This contains the scripts for Observer. Back up if you have created or modified a script.</td>
</tr>
<tr>
<td><strong>Windows Registry</strong></td>
<td>Using Regedit, export the following registry branch: 32-bit Windows operating system running any version, or 64-bit Windows operating system running version 16 or higher: HKEY_LOCAL_MACHINE\SOFTWARE\Network Instruments</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>Make note of the license information in . You need the contact/ department, company, identification number, and license number.</td>
</tr>
</tbody>
</table>
Index

Numerics
10 Gb Probe 21
10/100 network 77
25901 (port) 103
25903 (port) 103
32-bit 69
64-bit 51, 69
64-bit, RAM 69
802.11 5, 8, 13, 35
802.1Q 45, 105

A
active instance vs. passive instance 6
adapter speed 35
Adapter Speed tab 35
additional volumes, using 27
address tables 23, 110
Advanced Settings 78, 92
AES 32, 32, 45
alarms 8, 13, 103
allocating 72
analyzer connection 103
Anyone account 103, 103
Application Performance Analysis 49
Application Transaction Analysis 49
as probe or analyzer 49
ATM 27, 35, 36
auto-negotiation 75, 78, 92
SPAN port 75
autoupgrade 32
Autoupgrade tab 35
autoupgrading 32, 35

B
backup
installation 21
backups 23, 110
bad TCP checksums 105
troubleshooting 105
best practices 6
BIOS memory hole 69
Board ID 78, 92
broadcast traffic 27, 86
buffer 66
buffer size 6
buffer statistics 66
buffer, see capture buffer and statistics buffer 66
buffers 6, 8, 13, 13, 69, 70
capture buffer
64-bit Windows 66
Max Buffer Size 66
RAM limitations 66
size 66
capture card 34, 74, 78, 100
advanced settings 94
Advanced Settings 78, 92
auto-negotiation 75
Board ID 78, 92
current state 92
details 96
driver 95
driver requirements 17
events 97
general 92
passive probe instance 6
performance 6
probe instance warning 6
properties 78, 92
recommendations 72
resources 98
SPAN port, 10 Gb link 75
time synchronization 34
troubleshooting SPAN port 75
virtual adapters 80
capture card driver 17
capture decodes 35
CDU 35
Cisco 6xxx switches 108
troubleshooting 108
Cisco EAP/LEAP 50
clock synchronization 34
collecting data 34
collection interval 62
collision test 108, 108
common issues 102
common problems with 103, 103
network trending folder 32
probe name 32
configuring statistics memory 33
connecting 29
connecting to analyzer 28, 28, 28, 29, 34
content 40, 40
context 40, 41
contextual visibility 40, 41, 43
CRC-16 36
CRC-32 36
CSU 35
capture buffer 36, 36
D

D3 35
D3/E3/HSSI 35
data transfer 48, 48, 48, 48
daylight savings time 108
Daylight Savings Time 108, 108
decoding 8, 8, 8, 13, 13, 13
deduplication 8, 91
defining its purpose 72
defining probe as 80
definition 5
device manager 92, 92, 94, 95, 96, 97, 98
Discover Network Names 107, 107, 107
VLANs 107
DNS resolution 32
driver requirements 17, 17, 17
drivers 78
drivers, wireless 18
DS3
fractionalized 36
DSU
encapsulation 36, 36
dynamic traffic management 40, 40, 43

E

E1 35
WAN relay type 36
E3 35
fractionalized 36
EAP/LEAP 50
Edit Probe Instance 67
effects of packet capture 70
capsulation 35, 36, 36, 36, 36, 36, 36, 36, 36, 36
encryption 32, 32
AES 45
see also security 45
encryption key 21, 32, 50, 103
encryption keys 21
ErrorTrak 12
Ethernet 5, 5, 8, 35
full-duplex 8, 13
jumbo frames 35
Expert Probe 8, 8, 8, 13, 13, 32, 48, 48
as probe or analyzer 49
changing NIC 27, 86
configuring 35, 35
connecting to analyzer 28
data transfer 48
GigaStor 48
NetFlow 62
port bonding 59, 83
redirection 28
expert summary 8, 13

F

Fabric Manager 40, 40, 41, 42, 43
FIFO 42
FIFO buffer 43
filters 62, 62
filters, hardware 91
firewall, ports 103
fractionalized 35, 36, 36, 36, 36
frame check sequence 35
frame checksum 35
frame relay 35
frame size 35
Frame too large 35
full-duplex 8, 13
full-duplex Ethernet 8, 13

G

Gen2 capture card 100
Gen3 74, 74, 78
Gen3 capture card 100
General tab 35
Gigabit 8, 35
defining probe as 80
jumbo frames 35
Gigabit Probe 21
Gigabit tab 35
gigabytes 66, 66
Gigamon 40, 40, 41, 45
GigaStor 28, 42, 43, 48, 72
AES 32
collision test 108
encryption 32
Expert Probe 48
RAM 72
recommendations 72
reserved memory 72
traffic generation 108
virtual machine with 51
GigaStor capture 6, 8, 13
GigaStor Portable 108
GigaVUE 40, 40, 41, 42, 43
GigaVUE H series node 42

H

HA
See hardware acceleration 113
hardware 15, 67
hardware acceleration 72, 86, 87, 90, 91
hardware filters 91
hardware requirements 12
HSSI 35, 36
HSSI, fractionalized 35

I

in a switched environment 10
install 16
installation 16, 17, 17, 21
installer 16
installing 16, 17, 17
interface switching 8, 13
IP address
GigaStor 28
NAT 107
IP masquerading, see NAT 107
IP precedence 35, 35
IPv4 27, 27
IPv6 27, 27

J

jumbo frames 35, 35, 35

L
LAPB 35
laptop
NICS 50
using as probe 50
wireless 50
Layer 3 Switch 107
license 23, 110
license update 22
licenses
redeeming 21
troubleshooting 21
limitation of 49
load, preprocessor 6

MAC addresses 107
Mac Header 27, 27
matching between probe and analyzer 103
Max Buffer Size 66
megabytes 6
memory 67, 67
memory allocation 33
memory management 66
memory tuning 66
memory, see RAM 70
Microsoft 20
minimum specifications 15
minimum specs 15
mirror port 10, 80
mirror port, see also SPAN ports 10
mirror port, see SPAN 77
missing 104
missing from Observer 27, 86
moving through RAM 70
MPLS 8, 13, 24, 27, 27, 35, 35
ATM 27
IPv4 27
IPv6 27
Mac Header 27
pseudowire word 27
Multi Probe 8, 8, 13
changing NIC 27, 86
configuring 35, 35
connecting to analyzer 28
data transfer 48
limitations of 49
redirection 28
multicast 23, 110
multiple in a system 34

name, changing 32
naming 26
NAT 107, 107, 107
NetFlow 8, 13, 35, 62, 108
TAPs and 108
versions supported 62
NetFlow collector 62
NetFlow Trending collector 62
Network 1 probe instance 26
network adapter, see also NIC 27, 86
network card

Observer
no network card 27, 86
switching to probe 8, 13
system requirements 12
Observer Analyzer 21
Observer GigaStor 21
Observer Management Server 32
observer.exe 21
OMS 8, 13, 32
operating system 16
options 32
OSI Layer 1 & 2 errors
SPAN 77
OSI Layer 7 49

packet broker 42, 43
packet broker integration 42
Packet Broker Integration tab 40
packet capture 35, 35, 70
active instance vs. passive instance 6
buffer 66
daylight savings time 108
decoding 8, 13
GigaStor Portable 108
memory 67
RAM 70
packet captures
wireless 12, 50
packets
deduplication 82
moving through RAM 70
RAM 70
passive probe instance 6
performance 6
port bonding 8, 13, 59, 83
port tag 45
port Tx 94
probe connection 103
probe instance
active 6, 66
active vs. passive 6
assigning to adapter 80
best practices 6
configuring 35
configuring statistics memory 33
connecting 29
connecting to analyzer 34
defining its purpose 72
definition of 6
memory allocation 33
memory tuning 66
naming 26
passive 6
passive to active 80
redirecting 28
reserving memory 66
specifying NIC 34
virtual adapters 80
probe instance warning 6
probe instances
  redirecting 30, 88
  probe name 32
  probe redirection 28
Probe redirection error 103
Probe Service Configuration Applet 49
probes 30, 88
  Adapter Speed tab 35
  Autoupgrade tab 35
  autoupgrading 32, 35
  backing up 23, 110
  clock synchronization 34
  collecting data 34
  common problems with 103, 103
  configuring 32
  connecting to analyzer 28, 29
  D3/E3/HSSI 35
  definition 5
  encryption keys 21
  General tab 35
  Gigabit tab 35
  hardware 67
  hardware acceleration 72
  in a switched environment 10
  IP precedence 35
  MPLS 27, 35
  name, changing 32
  not connecting 103
  options 32
  port bonding 59, 83
  see probe instances 30, 88
  protecting 20
  running as Windows service 32
  security 30, 88
  software, versions 8
  SPAN ports 8
  statistics sampling divider 35
  switching to analyzer 8, 13
  T1/E1 tab 35
  updating 20
  upgrading 21, 21
  Virtual Adapters tab 35
  virtual TAPs 51
  VLAN access 103
  WAN 35
  wireless 35
  Wireless 802.11 tab 35
  see probe instances 30, 88
promiscuous mode 10, 12, 50, 51
protected memory 64, 67, 67, 67, 69, 70
protecting 20
pseudowire word 27, 27
Q
  QoS 35
  QSFP
  See SFP/SFP+ 116
R
  RAID 6, 6, 27
  RAM 15, 70, 70, 70, 72
    allocating 72
    buffer size 6
    effects of packet capture 70
    formula 66
    GigaStor 72
    limitations 66
    packet capture 6, 66
    see also buffer 66
    see also protected memory, user memory, and reserved memory 64
    recommendations 69
    reserving for Observer 35
    resizing 64
    statistics 66
    tuning 66
    used in Observer 64
    Windows 66
  RAM limitations 66
  RAM needed for busy networks 72
  Random Access Memory, see also RAM 64
  recommendations 69
  recommended specifications 15
  recommended specs 15
  redirecting 28, 30, 88
  redirecting, see probes 29
  redirection 28, 28, 28, 28
  registry 23, 110
  requirements, hardware/software 12
  reserved memory 8, 13, 67, 67, 69, 70, 72
  see also RAM 64
  reserved memory from 8, 13
  reserved memory in Observer 35
  reserving for Observer 35
  reserving memory 66
  resizing 64
  risks, SPAN 77
  RMON 10
  running as Windows service 32
  running Observer or Probe 49
S
  sampling divider 62, 62, 103
  scripts 23, 110
  security 8, 13, 30, 88
    encryption 45
    encryption key 103
    matching between probe and analyzer 103
    personal information 21
    Probe redirection error 103
    probes 30, 88
  self-optimizing management 40, 40
service 32
services 49
settings 10
sFlow 8, 13, 35
sFlow, versions supported 62
SFP/SFP+ 75, 78, 92
simultaneous 8, 13
Single Probe 8, 8, 13
  Anyone account 103
    changing NIC 27, 86
    configuring 35, 35
    data transfer 48
    redirection 28
    VoIP 49
Single Probe memory limit 67
slow 24
slow probe system 103
SNMP 10, 23, 110
SNORT 23, 110
software probes 8, 21
software requirements 12
software, versions 8
SPAN 80
  auto-negotiation 75
  risks 77
  VLANs 105
SPAN port 75, 105
SPAN port, 10 Gb link 75
see also mirror port 10
SPAN ports 8
  broadcast traffic 27, 86
  settings 10
  software probes 8
  see also mirror port 10
  virtual machine 51
SPANOSI Layer 1 & 2 errors
  OSI Layer 1 & 2 errors 77
specifications 15
specifying NIC 34
specs 15
statistics 35, 50, 66
  collection interval 62
  memory 67
  packet capture 35
  RAM needed for busy networks 72
  sampling divider 62, 103
statistics buffer 66, 66
statistics queue buffer 64, 67, 69, 70, 70, 72, 72
statistics sampling divider 35
storage 15
switching to analyzer 8, 13
switching to probe 8, 13
synchronization 34, 108
system requirements 12
system specification 15

T
  T1 35
    WAN relay type 36
T1/E1 tab 35
TAP
  NetFlow 108
TAPs and 108
TCP 107
TCP/IP 107
third-party capture card
  driver requirements 17
third-party hardware 15
time synchronization 34, 34, 108
Top Talkers 66
topologies 5, 8, 13
802.11 5
Ethernet 5
ToS 35
traffic generation 108, 108
transceiver
  See SFP/SFP+ 116
triggers 8, 13, 103
troubleshooting 105, 108
  analyzer connection 103
  bad TCP checksums 105
  Cisco 6xxx switches 108
  common issues 102
  probe connection 103
  slow probe system 103
  slow probe system 103
  virtual machine 51
users 8, 13, 103
  simultaneous 8, 13
using as probe 50

U
  updating 20
    Observer 21
  updating virus protection 20
upgrade 17, 17
upgrading 17, 17, 21, 21, 21
upgrading version 16 17
upgrading version 17 17
upgrading, encryption keys 21
user memory 64
users 8, 13, 103
  simultaneous 8, 13

V
  v16 17
  v17 17
  version 16 17
  version 17 17
  versions supported 62
virtual adapter 6, 35, 51, 59, 83, 86, 87, 90, 91
virtual adapter, probe instances 80
virtual adapters 80
Virtual Adapters tab 35, 80
virtual machine 12, 15, 51, 51, 51
virtual machine with 51
virtual NIC 51
virtual TAP 51
virtual TAPs 51
virtual TAPs 51
virus protection 20
VLAN 45, 105, 105
  “No VLAN” 105, 105
VLAN access 103
VLAN Statistics 105
VLAN Statistics tool 105, 105
VLAN visibility 107
VLANs 105, 105, 107
  Discover Network Names 107
  SPAN port 105
VM specs 15
VMONI 104
VMONI Protocol Analyzer 104
VMware 15
VoIP 8, 13, 35, 49, 49
VPN 107
vSphere 15

W
WAN 35, 35, 35
  fractionalized 35
WAN relay type 36, 36
WAN Type 36, 36
Windows 18
  32-bit 23, 69, 110
  64-bit 23, 51, 66, 69, 110
  registry 23, 110
  reserved memory from 8, 13
  reserved memory in Observer 35
  service 32
  services 49
Windows 10 16
Windows 2003 16
Windows 2008 16
Windows 2012 16
Windows 2016 16
Windows 7 16
Windows 8 16
Windows memory pool 67, 67
Windows protected memory 64
Windows updates 20
Windows Vista 16
wireless 5, 8, 12, 13, 35, 35, 50, 50
Wireless 802.11 tab 35
wireless access point 50
wireless driver 18
wireless network, encryption key 50
wireless packets, raw 12, 50

Y
YouTube 40, 40

Symbols
"No VLAN" 105, 105